SECURITY INFORMATION

ARMED FORCES SECURITY AGENCY

DF-292

52/52/SECRET/AFSA-14

Copy No. 1

From: AFSA-14

To: AFSA-14

[THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18, U.S.C., SECTIONS 793 AND 794. SEE ALSO PUBLIC LAW 513, 81ST CONGRESS, SECOND SESSION. ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW.]

Do NOT Destroy Return to the NSA Technical Library when no longer needed
S-3058
Copy

DF-292 52/52/SECRET/AFSA-14

THE CRYPTOLOGIC SERVICE IN WORLD WAR II

(German Air Force)

1. Attached is an Armed Forces Security Agency translation of a paper by Edwin von LINGEN on the Cryptologic Service of the German Air Force during World War II. A film of the document was received through CIA and a set of prints is filed in AFSA-144 under VO-106.

2. The author was in charge of the cryptanalytic work of the German Air Force against Russia and his paper offers valuable background material as well as some specific details regarding low echelon Russian systems.

3. Among other things von LINGEN devotes several paragraphs to the often discussed question of the degree of collaboration between the several German cryptologic agencies and points out ways in which a consolidation of the agencies of OKW, OKH and ObdL could have increased efficiency and cut personnel and expense.

4. In Part 3 von LINGEN offers a sample of "photo evaluation" (Bildauswertung) and states that he has some 400 photographs from Russia, Poland and Rumania which he is prepared to write up as Appendix to this paper. He has included 15 snapshots of Vinnitsa on the Bug as a sample of what he has in mind. While this material is not of great interest to AFSA some other agency may wish to acquire it.

Translated: R.W.P. 35 copies

June 1952 106 pages

Distribution: Normal

KJ 4738

CRYPTOLOGIC SERVICE
IN
WORLD WAR II
(German-Russian)

Edwin von LINGEN

Began: 1 March 1936

Ended: 5 May 1945

NOTE

Supplement I, in which all the snapshots from the East are evaluated and located, is still being worked on. It comprises some 400 different selected photos from all parts of the Soviet Union, Poland and Rumania.

In Part III of the report the city of Vinnitsa is shown as an example of pictorial evaluation.

Supplement I can be shown in connection with the report if desired.

This report is to be regarded as a draft. The detailed version of the report is yet to be written. All documents of the Russian Cipher Service (codes) have been destroyed or mislaid. However, they can all be reconstructed.

PREFACE AND EXPLANATORY NOTES ON THE RADIO INTERCEPT SERVICE

It is generally known that the individual troop units of the armies must maintain contact with one another in war as well as in peace.

In peace time, when the several troop units had stations which were in the main fixed, communication was carried on by wire, (telephone, teleprinter) or by courier post.

Only during grand maneuvers were orders, reports, etc., from the higher echelon to the troop units and between the troop units themselves, passed by radio.

In war time, when the troop units were in constant motion, they frequently had to change their locations and were far away from each other in the vast theater of war, and maintained contact with one another exclusively by radio.

To each troop unit was assigned a radio station which had transmitting and receiving apparatus by means of which it maintained radio contact with the adjacent troop units and received or sent necessary reports and commands. Each radio station had its own call signs and transmitting and/or receiving wave length which was known to the other stations with which it communicated.

If orders and reports had been sent by radio in plain text, they could have been intercepted and evaluated by anyone, whether friend or foe. To avoid that, the important reports and commands were encrypted by means of a code which was prepared at a central cryptographic unit, i.e., the text to be transmitted was replaced by digits according to a code and was then radioed in those digits. For this purpose each radio station had especially trained cipher personnel. These code clerks were responsible for the correct encipherment and decipherment of the texts.

All reports and commands of the enemy that were sent by radio were intercepted by the other side. For this purpose special receiving stations were set up which picked up all radiograms of the opponent.

Enciphered radiograms went to a section (located at each radio receiving station) and were there given special treatment, i.e., an attempt was made to decipher the text of the radiogram from the groups of numbers. This unit then was concerned with decipherment of the radiograms and hence of the code by which the text had been encrypted.

To clarify some expressions which appear frequently in the report certain points will be taken up here.

The central unit of the German Air Force which directed all the radio intercept service was called the "Chiffrier-Stelle". It really should not have been called thus because it was concerned exclusively with decipherment and evaluation of intercepted radiograms of the enemy and had nothing to do with encipherment. The duties of this Chiffrier-Stelle included the preparation of various codes, encipherment tables and cryptographic materials by which radiograms could be enciphered.

The radio intercept service merely received messages which the enemy sent by radio, deciphered the enciphered messages and evaluated the deciphered text. The deciphered and evaluated reports and commands of the enemy were called "V.N." = confidential reports*; because they did not come from agents and could be regarded as completely confidential. The reports which were brought in by agents (espionage) could not always be regarded as completely confidential since they did not come directly from the enemy as did the enciphered radiograms. Agent reports and intercept reports came from two different sources of information and were utterly different in their nature. During the war it was possible to get better and more reliable information regarding the enemy, his movements, intentions, supply, strength and character of the troops through the intercept service than through actual espionage.

Even in peace time every country was trying to gather all kinds of information regarding its immediate neighbors. This did not necessarily mean preparation for war, but it was done for security reasons. These bits of information were gathered in different ways. Every country that

* Translator's note: Others interpret V.N. as Verlässliche Nachrichten = reliable reports.

was always open for foreign travel would always afford every other country the possibility of getting a picture of its cities, streets, bridges and even individual factory installations, etc. Only in a rare case could this be done in the Soviet Union. For 20 years (figuring down to 1939) the Soviet Union had been separated from the rest of the world by an Iron Curtain and only very few photographs of this country reached other countries. Not until the German-Russian war, when German troops penetrated far into Russian territory and countless photographs came into the hands of German official agencies, was it possible to form an idea of this peculiar country by evaluating these photos. Using the many pictures taken during the war, including both those taken by air reconnaissance and those by the ground organizations, it was possible to put together a so-called pictorial atlas which contained not only the associated air photographs but all other pictures of cities, streets, bridges, character of the soil and major features of the landscape. These pictures were carefully coordinated with maps, and evaluated, yielding a pictorial atlas such as had never been attempted before for a country like the Soviet Union.

In my report I should like to treat primarily three areas which afford a survey of

1. The radio intercept service of the German Air Force,
2. The radio and cipher service of the Red Army, and
3. The evaluation of the pictorial documents from the Soviet Union.

I shall not attempt to compose my report on a scientific basis but shall try to explain the several subjects as simply as possible.

The experts in the radio intercept service who were occupied primarily with the East displayed their special talents during the entire campaign in the East down to the final day of the war in untiring positive effort and their success in creating a mosaic was deserving of recognition. Since they were dealing with secrets of the first order, they performed their valuable work without fanfare so that only a very small circle knew anything about it and they remained unknown heroes.

It is not saying very much to call them unknown heroes because by their hard mental labor they helped their comrades at the front in many ways. By their swift decipherment of important enemy radiograms they were able to avoid heavier losses among their comrades, to keep them from being encircled by the enemy, and they would have avoided the catastrophy of Stalingrad if the German Command had acted properly on the basis of their prompt reports. These unknown heroes did their duty day and night because they were convinced that they were fighting like their comrades at the front, only with a different weapon. And this weapon could be powerful and effective if it had been properly recognized and utilized by the higher echelons. Through its efforts the intercept service was able to reveal the activity of the Red Army in many ways both before and during the war. This was the chance such as had never been afforded before. I hardly believe that any foreign power will again succeed in learning through its intercept service as much regarding the Red Army because we must definitely assume that since the war the Russians have learned a great deal regarding the valuable results of the German Intercept Service and have remade their own radio and cipher service completely. The errors and the frivolity of which they were guilty down to the very end of the war they will probably not repeat. And should that be the case, then the cryptanalysts of the future will have a hard task and will hardly be able to solve their problems 100% as was done down to the end of the war.

CRYPTOLOGIC SERVICE IN WORLD WAR II

Part I.

Setting up the Cryptologic Service in the German Air Force.

Although there had been a well established cryptologic section with numerous outstations (intercept stations) in OKW since 1923, the then young German Air Force did not start to set up similar stations until 1936.

In spite of the warning by OKW and in spite of its suggestion to combine the cryptologic units of the three branches of the armed services, the High Command of the Air Force resolved to make itself entirely independent of the army in this field and dispatched its interpreters to the fixed radio intercept stations of the army. These interpreters were to receive the necessary instruction in cryptology from the Army as long as the Air Force should not have set up its own intercept stations so that they would be able to function independently with their own stations.

Each army intercept station worked by itself and in the main quite independently. They received important instruction from the intercept control center (Chiffrier-Stelle OKW) and had to send their final results to this station regularly. The army intercept station was divided into four separate sections:

1. Receiving station (with 12 to 15 receivers),
2. Traffic analysis,
3. Content evaluation,
4. Cryptanalysis.

Like the operators, all the evaluators and cryptanalysts were civilian employees. Only the head of the station and the administrative personnel were in the military service. The several sections worked absolutely separate from one another and the cryptanalytic section was particularly secret and carried on its work in the main without the knowledge of the other sections.

The 12 to 15 receivers were divided between day and night duty and intercepted the radio traffic of the Red Army. Each receiver was

assigned its range (frequency range) beyond which it must not go. The single ranges overlapped so that there could be no gap in the reception. One or two receivers were always employed for such purposes. but had to notify one another of results to avoid duplicate interception. Each army intercept station had its own intercept area: Northern, Central or Southern Sector of the Russian traffic.

Reception as a whole was directed by Traffic Analysis which received instructions from Content Evaluation and Cryptanalysis to supplement its own observations.

The chief duties of Traffic Analysis were:

1. Interpretation of call signs and frequencies of the Russian radio stations.
2. Interpretation of operational signals in Russian procedure traffic.
3. Organisation of the intercepted networks and its evaluation.
4. Reconstruction of tables of frequencies and call signs.
5. Evaluation of Russian traffic on the basis of interpretations made.

Even before the war some 90% of the intercepted Russian messages were enciphered. The remaining 10% were sent in clear. These clear messages were mostly weather messages or pure procedure traffic between single stations. The enciphered messages were received in groups of 2-, 3-, 4- or 5- digits and were worked on by the cryptanalytic group. The decrypted messages, with the Russian text entered thereon, were then passed to the Content Evaluation Section. Here the decrypted messages were translated into German and a V.N. report was compiled daily from the intercepts. Content Evaluation also carded all troop units mentioned in the messages, all places, names of commanders and other significant data, and in connection with the Traffic Analysis Section passed its reports to the next higher unit, in this case OKW/Chi.

After eight months of general instruction at the army intercept station and after successful practical work in cryptanalysis I was called to the newly established Chiffrier-Stelle in the Air Ministry where I was given the desk "Entzifferung-Ost".

Late in 1936 the Cipher Section in RLM, which was then called the 7th Section of the General Staff, began to work independent of the Army. At the same time the three intercept stations of the Air Force were set up: 1. Königsberg, 2. Breslau, 3. near Berlin.

These three outstations, disguised at that time under the name "Wetterfunk-Empfang-Stellen" (weather stations), began working with their hardly trained personnel and tried to intercept only Russian Air Force traffic. At that time this was relatively easy. The Russian Air Force sent its radiograms in two- or three-digit groups and the call signs differed considerably in structure from those of the Army. Only part of the intercepted messages could be decrypted at the outstations because the cryptanalytic personnel had scarcely any experience in this field and was solving only the simplest ciphers (Cäsaren). The undecrypted radiograms were sent currently to the Chiffrier-Stelle RLM.

Since from this point on, I was in charge of all the cryptanalytic work against the East and was made responsible for the course of decryption both at the Chiffrier-Stelle of RLM itself and at the three outstations, I shall describe primarily this type of work in my report. However I shall not stick to cryptanalysis but shall also touch upon anything which had to do in any way with the cryptologic service.

In order to report on the extensive work of the Chiffrier-Stelle, I should like to give first a short survey of the organization and build-up of the cryptologic service.

The main cryptologic unit, which had its seat in the Air Ministry, was as a whole subordinate to the Chief of the Air Signal Service. It was subdivided into four desks or groups.

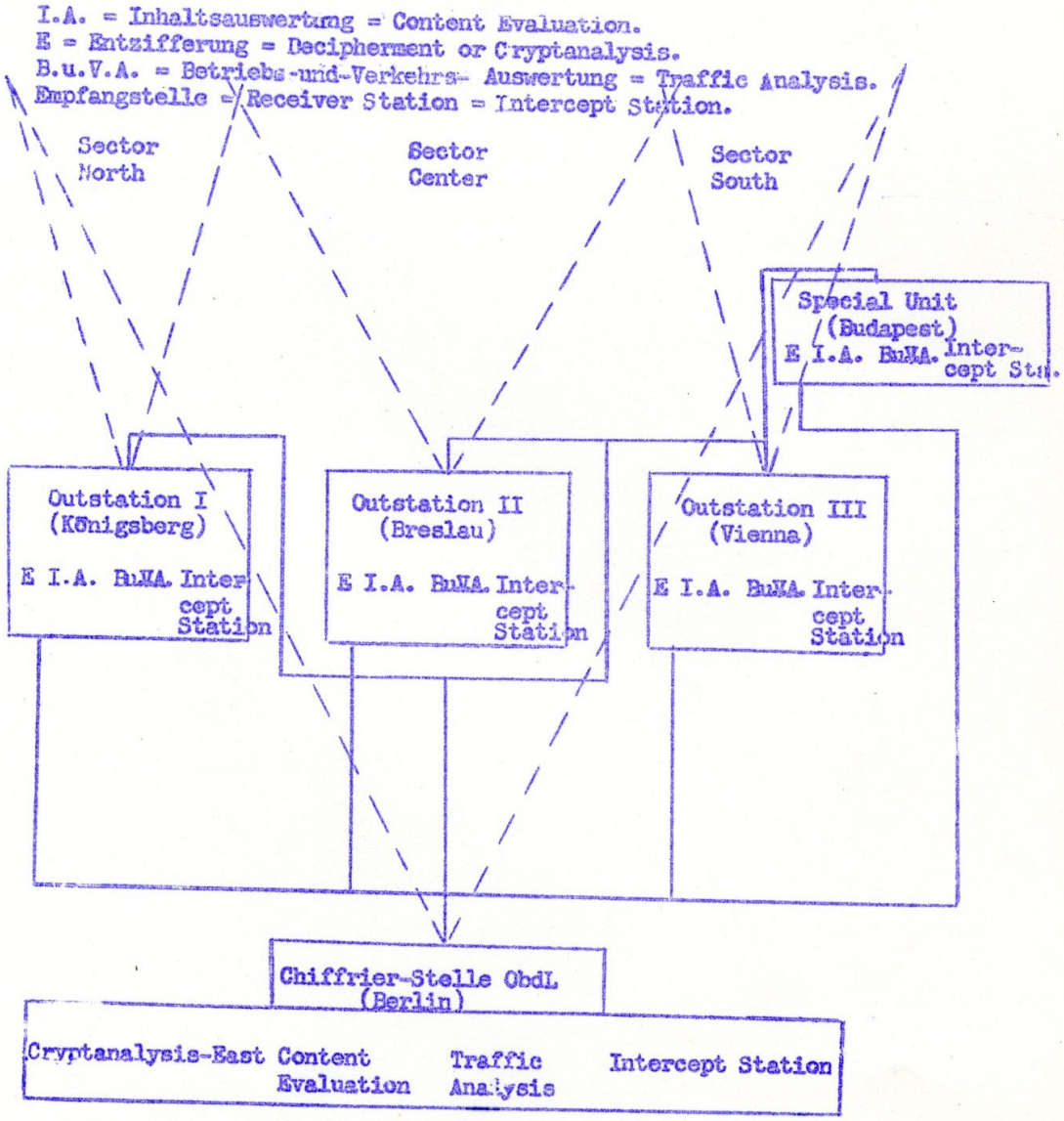
1. Cryptanalysis.
2. Content Evaluation.
3. Traffic Analysis.
4. Intercept stations.

While the intercept stations consisting of 12 to 15 receivers were housed with the other groups at each outstation, the intercept station of the Chiffrier-Stelle RLM was located in the vicinity of Berlin.

Each outstation was assigned its work range, beyond which it was not permitted to go, and was supposed to work quite independently as far as possible and to send its VN's and its traffic reports to the Chiffrier-Stelle and also to the competent Air District Command.

All the intercepted traffic from all four intercept stations was worked on at the RLM Chiffrier-Stelle and the results were imparted to the three outstations. This resulted of course in some duplication of effort which could not be avoided but which served very well as a control and for correcting mistakes.

Sketch of the several work areas.



The function of the Cryptanalytic Section of the Chiffrier-Stelle in the Air Ministry consisted not merely in picking up and guiding all the cryptanalytic effort directed against the East and in decrypting systems not solved by the three outstations, but also in instructing the newly established outstations of the Air Force in all matters and in training the personnel in accord with experience gathered. The newly recruited personnel had to be given the proper introduction to cryptanalysis in order to be able to perform independently in the course of time the problems which would be encountered.

After the incorporation of Austria the third outstation of the Air Force moved to Vienna and a camouflaged secondary station was set up in Budapest. This special station in Budapest was manned by personnel selected by the RLM Chiffrier-Stelle (Germans in civilian clothes) and worked in close contact with the Intelligence Service of the Hungarian Ministry of War.

Thanks to the well developed communication network between the RLM Chiffrier-Stelle, the three outstations and the special station in Budapest, the Chiffrier-Stelle received copious traffic in the speediest fashion and was able to do its cryptanalytic work better and more precisely.

After the Air Force had established its own intercept and cipher service, any help from and any insight into the secret branch of OKW/Chi was at first generally made very difficult. The rivalry of the three branches of the armed forces and later when the High Command of the army (OKH) had set up its own cryptologic unit in Berlin and thus made itself independent of OKW/Chi - a bitter rivalry existed between these two cryptologic agencies. It is only due to the fact that I was well acquainted personally with the directors of the cryptologic agencies of OKW and OKH that it was possible to establish a fairly close contact and to reach a positive collaboration and an exchange of experiences and of solved systems. This informal understanding and collaboration also made it possible for me to get a full survey of the cryptographic systems of the Russian Army, Navy and Border Guard (NKVD).

INTERCEPT SERVICE OF THE GERMAN AIR FORCE

In January 1937 the newly established Chiffrier-Stelle RLM began working initially with a few people. The entire cryptanalytic personnel had little or no training, had no practical experience, and initially worked more according to their hunches than on any professional basis.

Luckily the Russian Radio and Cipher Service was also being developed at the same time. Before I pass on to the central work of the intercept service of the German Air Force, I should like to give a short report on the structure and activity of the Russian radio communications.

All units of the Red Army in European Russia were divided into several military districts (VO = Voenyj Okrug): LVO = Leningrad Military District, MVO = Moscow Military District, KVO = Kiev Military District, KhVO = Charkov Military District, etc. The radio stations of the various units communicated with one another by radio only within their military districts. Each military district had its own systems of call signs and wave lengths. Even on the basis of different types of call signs one could determine whether an Army or an Air Force station was involved. The Army stations usually used four to five letter call signs. The Air Force, on the other hand, had three place call signs (3 letters or 2 letters and a digit). Call signs were changed daily both in the Army and the Air Force.

The Russian radio stations communicated with one another in various fashions:

1. Star traffic,
2. Link traffic
3. Circular traffic which had a varying number of stations.

To each radio station was assigned a cipher officer and to the radio control station a cipher section. They were responsible for seeing that all tactical and important radiograms were sent enciphered. They got their instructions as well as their cryptographic material from the main cryptographic center in Moscow and had to follow precisely the instructions for the use of the several codes and ciphers. But that this was not always the case will be reported elsewhere.

Like the call signs and frequencies, the keys to the several codes changed daily. The change took place at midnight Russian time either according to system tables issued for a week or ten days or else the call signs, wave lengths and keys for the new day were announced in an enciphered message or sent by courier.

For internal traffic of the various stations of the Red Army (i.e., for army and air force) a uniform "conversation table" (Peregovornaya Tablitsa) was used. The regulations, issued by the cipher section in Moscow, stated that the use of this table was permissable only for procedure messages between the several stations and for practice purposes in enciphering messages of immaterial content. However, this rule was often overlooked by the personnel, they sent their tactically important messages quite often in this simple substitution, whereupon a strict reprimand came from above.

This "conversation table" was simple in structure and in encipherment and could be solved in a short time and its basic form recovered. (For details see Part II).

Since the rule against enciphering important and secret material with the above mentioned table was frequently disregarded and Russian radio stations frequently requested one another to send through the keys for the day, the decoders at the German Chiffrier-Stelle frequently obtained new keys in this fashion and could decrypt the intercepted messages quickly and easily.

This violation of security on the part of Russian radio personnel was observed often during the war. It was impossible to determine precisely whether this was due to frivolity or to a primitive quality of the Russian personnel which was just then in training. Instruction from above did not seem to have much effect on the Russian radio personnel because the same mistakes were made over and over again.

Tactical commands and military pronouncements of the ground organizations of the Russian Air Force were sent enciphered in an Air Force code. Before the war only one Air Force code was in use at one time for military districts.

Such an Air Force code was generally changed just before the Autumn or Spring maneuvers.

The main cipher section in Moscow usually issued such a code two or three weeks before the beginning of the maneuvers, so that the personnel could become familiar with the code. In this pre-maneuver period messages enciphered in this code with insignificant content were exchanged by all Russian stations which were to participate in the maneuvers. At this time the German intercept stations had to pay special attention to all traffic which used this new code so as to pick up plenty of messages. Since enough message material was received, the cryptanalytic section at the Chiffrier-Stelle of RLM was able to solve the newly introduced Air Force code relatively quickly. The deciphered code was then reconstructed, reduced to the basic code, the decipherment was recognized along with its changes, and before the maneuvers began, the first documentary materials were sent to all outstations after which the intercepted traffic was decrypted immediately at the outstations.

Maneuvers of the Red Army in Radio Traffic.

The entire maneuvers of the Red Army with its Air Force could be followed very precisely by the intercept service. During this time much information and much experience would be gathered by the German cipher units. The German operators learned to know the fists of the several Russian stations and were able to recognize them again in spite of changes of call sign and frequency. The Traffic Analysis Section interpreted the various links and networks, compiled new call-sign tables which were based on a specific system and were also able to identify new Russian stations. The Cryptanalytic Section could do good work with the abundant material, the code was recovered and the deciphered messages were read almost 100%, the recovered groups of the code were sent currently to all outstations and the texts of the messages were carefully studied. (Structure of such an Air Force code is shown in Part II). Content Evaluation was able to follow the entire maneuver by the solved messages and composed a comprehensive report. All names, places, types of planes, etc., were carefully carded.

These Air Force codes were rather simple in structure before the war, contained at most only ten pages with 100 lines each, hence such a code could contain at most 1,000 different groups, i.e., letters, digraphs, words, sentences, numbers, punctuation marks, types of planes, compass points, places and troop units. In spite of the fact that there were quite a few words in such a code which might have been used by the Russian cipher personnel, the text of the messages was usually made up of letters. The text which was for the most part made up solely of letters reveals, as is well known, the frequency of the single letters which have been expressed in digit groups and is easily solved on the basis of a count. The words which then appear sporadically in the text could be guessed by the context. So, although these codes when properly employed could afford sufficient secrecy, they were used in a very primitive fashion and could be solved in a very short time.

It was possible to recognize the beginning of the maneuvers by the increased radio traffic and the large number of messages. Hardly any plain text was transmitted during maneuvers. Even weather messages and location reports were sent enciphered by special weather codes and system tables.

During the maneuvers of the Red Army there was a constant exchange of experiences, observations and interpretations between the cipher sections of the Air Force, OKW, and OKH, whereby the Army as well as the Air Force compared and exchanged new types of solved systems. Among other things this made it possible to recognize that Russian radio and cipher personnel were still in training and had a great deal to learn.

Aside from the usual Autumn and Spring maneuvers, there were simple theoretical exercises in the intervals between. In connection with these simulated maneuvers many messages were exchanged. A certain percentage could be regarded at once as pure training traffic. These messages contained either at the beginning of the digit group the indicator "UCh" (Uchebnaya = practice message), or they were characterized by digits in an ascending or descending sequence.

For example: 345 678 901, or 7654 3210 9876, etc., or groups of like digits appeared: 2222 5555 0000. These groups of like digits occurred scattered through the entire message and attracted attention by their frequent repetition so that the messages could be recognized at once as practice messages.

Such practice messages were transmitted merely for practice in sending, contained nothing but arbitrarily selected groups of digits and were quite meaningless. Our operators had to pay attention when they picked up such immediately recognizable practice messages. As soon as they recognized them, they were to stop intercepting and pick up other networks which were carrying real traffic.

Another group of radiograms which could also be characterized as practice messages involved messages with enciphered text. These, when deciphered, revealed thoroughly military character. They contained orders, reports on enemy movements with place data, unit designations, unit movements, delays in supply and other tactical matters.

When these enciphered messages were first intercepted and decrypted (they were all enciphered by the code momentarily in use), it was assumed initially that local maneuvers of separate troop units were involved. But when in the course of time the same texts reappeared word for word, enciphered in a different code, it was recognized that these were make-believe maneuvers. This exercise was carried out therefore not merely to give the operators practice in sending but also to train the code clerks. For training purposes tactical texts had to be enciphered well and quickly and at the same time the sending of the operators could be rechecked.

Since before the war all decrypted messages were carefully assembled in the RLM Chiffrier-Stelle, there came into being in the course of time a so-called reference work which the cryptanalyst often used when they wanted some striking expression in their work on a new code. Thanks to the collection of tactical practice messages a new Air Force code could be solved and worked out in a brief time. In connection with the initial solution of these new codes certain sentences and place names attracted attention. After the old messages had been studied it was learned that this was probably the same text.

On the basis of the count made of the new messages the text of the old messages was inserted in the new messages on the basis of frequencies. The assumption was fully confirmed and the new code was quickly and completely solved. This example showed clearly the possibilities with which the cryptanalyst can count and what ought not to be done to facilitate the betrayal of his systems to the enemy. Such and similar examples were repeated during the war.

Training of Cryptanalytic Personnel

In the period between the maneuvers of the Red Army, when radio traffic was in general quiescent, practical use of the time was made in the cryptanalytic section of the Chiffrier-Stelle HLM and at the three outstations. The cryptanalytic personnel, which was constantly being reinforced, was given additional training in courses given by myself. All the traffic which had already been decrypted was worked through once more, the solved codes were filled in still further and all the results were evaluated.

To these cryptanalytic courses, which were held at the Chiffrier-Stelle in Berlin, all the cryptanalysts of the three outstations came in turn. The individual courses lasted about four weeks. The men had to encipher the texts themselves. As models they had the previously solved codes both of the Air Force and of the Army. In this way they learned to recognize new types of codes and of encipherments and also learned the correct way of enciphering texts. The texts used for these exercises were the Russian practice texts mentioned above. These were to be deciphered in good workmenlike fashion by the participants in the course. They knew neither the code nor the encipherment used for these texts. In this practical work the members of the course could see for themselves how little thoughtless errors in encipherment facilitate the work of the cryptanalyst.

The members of the course were instructed only in Russian ciphers. First they were taught the most elemental concepts of cryptanalysis using simple substitution tables.

When they had had enough practice with these and had mastered the logical steps of decipherment, more difficult types were attempted.

Since at the beginning of their activity these people could not distinguish between the solution of a code and its decryption, it was necessary to impress this upon them so as to facilitate decryption in general (decipherment and recovery of the basic code, see Part II).

The Russians had a fondness for all types of system tables. They set up tables of call signs, frequencies and keys by which they could without question work well, quickly and simply, but by means of which they also facilitated the work of the enemy's intercept service. Once these system tables for encipherment of the codes had been recognized by the German cryptanalysts, special value was attached to their recovery since with them it was merely necessary to decode the intercepts without solving them.

The cryptographic systems received from OKW and OKH, i.e., pure army codes, were also worked through in these courses. In this way the Air Force cryptanalysts became acquainted with other types and systems which stood them in good stead later on.

In these three years before the war the cryptanalytic unit of the Air Force, thanks to its self-training and new methods, caught up with the unit of the army, which was already fifteen years old, and was able to work independently and not without success on its own.

The employment of the intercept service in the Army and Air Force was different before the war. Even in the matter of training the newly recruited cryptanalytic personnel by giving courses no general introduction to traffic analysis was given at the army stations. On the one hand, all decipherers of the Air Force worked in close connection with the various evaluators and, on the other hand, the evaluators got a survey of current work in cryptanalysis so that each helped the other with supplementary information and suggestions for simplifying the job as a whole. In the Army these fields of endeavor were strictly separated from one another. According to the regulations, the evaluators must not

be initiated into the work of cryptanalysis and the cryptanalysts never got any exact information regarding the results of evaluation. Later on the army took over to some degree this close collaboration of the several fields of the intercept service, but only to a degree, and this separation of the several fields resulted in a certain disadvantage which was recognized even by the intercept service of the army itself.

Moreover, the constant struggle for existence, rivalry and a desire for prestige between the two cipher units of OKW and OKH led to a dispersion of the few good cryptanalysts available. Since the cipher section of OKH had made itself completely independent and taken over control of the army intercept stations (outstations), the cipher section of OKW, since it had no intercept stations of its own and was left without traffic, was practically put on ice or was dependent on the good will of Chiffrier-Stelle OKH. The army unit was delighted at having put OKW/Chi on ice so that it had to spend its time on Archive material and was not ready to admit that the well trained capable cryptanalysts of OKW were really idle. Only because I was personally acquainted with influential parties in both units was I able to bring about "peace" by arranging for close cooperation between the three agencies and to get all the cryptanalytic talent back on productive work.

Development of "Entzifferung-Ost"

In the three years before the war the Cryptanalytic Section East of the German Air Force developed in a perfectly natural fashion. In order to pick up all the traffic on the Russian Air Force networks the intercept stations had to get more receivers. The frequency ranges monitored were worked over more precisely and subdivided, the search for hitherto undetected traffic was intensified, and so the number of intercepts increased automatically.

The three outstations of the Chiffrier-Stelle RLM (Königsberg, Breslau and Vienna) were assigned intercept areas beyond which they were not to go. All radiograms not deciphered at the outstation were forwarded

currently to the cryptanalytic section of the Chiffrier-Stelle RLM. It in turn sent to the outstations the codes and systems of encipherment which it solved. All newly interpreted groups of the codes in use as well as all types of encipherments were supplied to the cryptanalytic units of the three outstations so that completion of the code resulted simultaneously in all the cryptanalytic units.

At certain intervals of time I or my representatives visited the three outstations and checked to see whether the cryptanalytic sections were doing their work in the same way it was done at the central unit. The heads of the cryptanalytic sections of the outstations were also summoned to the Chiffrier-Stelle RLM from time to time so that they could follow the cryptanalytic procedure and its organization so as to conduct their work in the same way.

This uniform procedure, which I suggested and put through, turned out later during the war to be very practical and useful.

In the course of time I worked out in our own cryptanalytic unit a precise delineation of the several fields because the manifoldness of the work required it and the personnel had to accustom themselves to specialized tasks.

The entire cryptanalytic unit at the Chiffrier-Stelle RLM was divided into the following groups:

1.	2-digit groups	Handled all messages transmitted in 2-digit groups = Cäsaren.
2.	3-digit groups	Handled all messages transmitted in 3-digit groups = code books.
3.	4-digit groups	Handled all messages transmitted in 4-digit groups = code books.
4.	"Neu-Entzifferung"	Handled all unsolved new codes and encipherments and recovered the basic form of the code.
5.	"Ausarbeitung"	Worked on solved codes using the accumulated traffic. [to complete recovery].
6.	"Planquadrate"	Merely worked on those types of enciphered coordinates which occurred in enciphered messages.
7.	Search and identification service	Surveyed the solved codes and maintained a card file of places, names, troop units appearing in messages.
8.	Business office	Recorded Top Secret documents and conducted correspondence.

To each group was assigned a specialist, the best cryptanalyst or expert, who was made responsible to me for the fast and satisfactory functioning of his group. Each group head was free to make improvements

in the working process, to try out and employ new methods for more rapid and easier decryption of the messages. If these experiments turned out well in practice they were also introduced at the outstations.

The control of the cryptanalysis as a whole at the Chiffrier-Stelle RLM and at the three outstations was centralized in my hands. My superior at the Chiffrier-Stelle and the Chief of the Air Force Signal Service, who understandably enough had no particular knowledge in the field of cryptanalysis, placed full confidence in me and gave me a free hand. What they asked of me was that the cryptanalytic effort East should function satisfactorily both at the Chiffrier-Stelle and at the outstations. The internal organization was entirely my affair. The instructions which went to the cryptanalytic units of the outstations were prepared by me but had to be signed by the Chief of the Chiffrier-Stelle RLM. Directions and instructions given by telephone or by teleprinter and changes in working methods were transmitted by me independently to the outstations and later laid before the Chief of the Chiffrier-Stelle as a matter of routine.

In this way it was possible to achieve expert rapid work in all the cryptanalytic units of the Air Force for which I alone was responsible. I was also given absolute freedom in respect to collaboration with the cryptologic agencies of OKW, OKH and OKM.

All undeciphered radiograms which were passed to the Chiffrier-Stelle by the outstations were worked on by the appropriate groups of the Cryptanalytic Section of RLM. If these messages could not be deciphered, they landed ultimately on my desk. I alone was permitted to decide whether these undecrypted messages should continue to be collected or, when no more were coming in, should be destroyed. In this way we avoided having outstations and the cryptanalytic groups at the Chiffrier-Stelle laying aside undeciphered messages or destroying them and we were forced to work over the intercepts more thoroughly.

General Survey and Procedure

All Russian radiograms copied by the receivers came first to the Traffic Analysis Section. This group which was concerned with the interpretation of call signs, procedure signals, frequencies and consequently with the several radio networks, made its notations if it knew which call signs belonged to this or that unit. If the units were known, they were entered in red against the corresponding call signs. Moreover, the individual messages were sorted by networks and links and passed to the cryptanalytic section.

All radiograms (enciphered) whether from its own intercept station or from one of the three outstations came in the cryptanalytic section first to the group "search and identification service". They were first sorted according to the different types of message groups within the links that had been identified, having regard for the loss of time, and it was determined which links could be solved by which already solved codes.

The "Search Identification Service" kept a double card file. Every code solved in Entzifferung-Ost was given a serial number, e.g., RC. 35-3 or RC. 36-4, i.e., Russian Code Number 35 enciphered in 3-digit groups and Russian Code Number 36 enciphered in 4-digit groups. The 2-digit systems (Cäsaren) were designated C.T. = Cäsaren-Tafel plus the serial number. Each code number had its own card in the file on which was entered the unit (troop unit) which used this particular code. Furthermore there were entered on this card the call signs with which the stations of this unit developed their traffic with other units. The second file was arranged by troop units. Each troop unit had its own card on which were entered all code numbers used to encipher its traffic. Consequently when the Traffic Analysis Section, in going through the intercepts, had interpreted the call signs and appended the troop unit in red, it was possible to look up this troop unit in the card file of the "Search and Identification Service", find the code number and note it on the message. After being thus sorted, the messages went to the groups which worked on 2-digit, 3-digit and 4-digit messages.

Messages which were given no code number by the "Search and Identification Service" had to be checked very precisely by the experts of the various cryptanalytic groups. There was a possibility that the call signs had been changed and that the Traffic Analysis Section could not yet interpret the change. But since the codes and encipherments which were currently being worked on were familiar to the cryptanalysts, it was possible to identify the codes and hence also the troop units. When this was the case, the cryptanalysts passed their observations to the "Search and Identification Service". There the change of call sign was noted in the card file and notice given to the Traffic Analysis Section which in turn undertook further interpretation and the setting up of the network.

But when messages could not be recognized by the cryptanalyst and a count showed that a new code was involved, these messages were passed to the group "New Decryption". The same thing happened with those messages which were given a code number on the basis of the call sign but could not be read by the code noted. In such cases the unit had put a new code into use and it would have to be newly broken.

This discovery was also passed to the "Search and Identification Service" which made an entry in its card file and passed the information to the Traffic Analysis Section.

Aside from the card files mentioned there was set up in the "Search and Identification Service" "a warrant for arrest" (Steckbrief) for each code. It was a little book with several pages. On page 1 was the designation of the unit. On page 2 were entered all the code numbers which had hitherto been used for this unit and been solved by the cryptanalytic unit. On the next page were listed place names, names of commanders and of other troop units found in the solved messages enciphered by the code of the unit in question.

When "New Decryption" received messages of a radio link for study it called upon "Search and Identification Service" for the "warrant" of the troop units concerned. It pulled all the codes listed as having been used by this unit and compared their type, structure, system and encipherment with the count that had been made of the new code. It could be assumed

definitely that place names and signatures (names of commanders which were usually enciphered in letters or digraphs) would appear in the same traffic with the new code. The cryptanalyst could find all these characteristics in the "warrant" and thus obtain help in the solution of the new code.

When it was impossible to determine from the traffic which had to be decrypted the troop unit to which the new code belonged (unknown call signs), the cryptanalysts had to start work without these characteristics. Once the first interpretations had been made (these were generally addresses or signatures), then they could inquire of the "Search and Identification Service" regarding the troop unit where the newly interpreted addresses or signatures occurred.

In the card file of personal and place names, which was also maintained in the "Search and Identification Service", there were entered behind the name or place name the troop units which had mentioned these names or places in their radiograms. Then the "warrant" could be used to facilitate further solution.

The replacement of an old code by a new one or the identification of the troop unit involved on an unknown link was reported immediately to the Traffic Analysis Section. Thereafter all additional messages could be marked with the troop unit and further identification of the radio network could be undertaken. This close collaboration saved a great deal of time and speeded up the decryption of the messages and the identification of the radio nets.

After "New Decryption" had solved the new code, i.e., when they had gotten to the point where they could produce a text even though not a perfect one, and after they had reduced the solved code to its basic form and recognized the system of superencipherment, this code would go to the group doing current decoding. This group would then handle currently incoming messages and enter the text above the cipher numbers.

The newly solved code was assigned a serial R.C. No. by the "Business Office" and this was immediately announced by teleprinter to the outstation in whose area this traffic originated.

With this the case was settled as far as "New Decryption" was concerned. Further work on the code, which of course still contained many unrecovered groups (syllables, words, etc.), was done in the group "Ausarbeitung". This group received all the traffic that had already been partly deciphered in the new code and worked over it conscientiously until the messages yielded good text and numerous new groups were recovered.

New recoveries when first guessed in this group were entered in the code in pencil. When these new recoveries had been confirmed by other messages they were entered in red and were considered 100% correct. New recoveries found while working on the code were entered on a slip by the worker. These were sent to the several groups of cryptanalysts who were working on current traffic in the new code and needed these new groups urgently to complete their decodes. Moreover all new recoveries were reported by teletype to the outstations in whose area the newly solved code was in use.

To facilitate completing the recovery of the code, all syllables and words that were definitely identified were entered alphabetically in a list. In this list it is necessary to include in alphabetic sequence not merely syllables and words but also digraphs, sentences and other typical items which occurred in the enciphered messages. This yielded a reference work of some 20 pages with 100 elements to the page.

Whenever in the solution of the new code a numerical group stood opposite an empty cell and before or after this cell several words had already been entered, it was possible to look up in the reference work the appropriate syllable or word which would both fit into the alphabetic sequence and make sense in the message text.

This reference work was also supplied to the outstations who worked on their codes by the same methods and were able to improve the already solved codes. Every new interpretation, every solution of a code and identification of keys was to be passed by the outstations to the Cryptanalytic Section of the Chiffrier-Stelle. Codes solved by the outstations were assigned a serial number by the Chi-Stelle (Cryptanalytic Section) and were passed to the group "Ausarbeitung" for further work.

In the group "Ausarbeitung" there was a group of people who spoke Russian perfectly. These experts did not need to be specialists in cryptanalysis. They received the already solved codes, all superencipherments that fitted in with partially solved messages, and merely had to complete the text of

the messages through their good acquaintance with the Russian language. For this it was not enough to have a good knowledge of the Russian language, they also had to be well acquainted with the special terms used in the Russian cipher service.

The remaining decipherment groups which were concerned primarily with current decoding and with the solution of relatively simple easy codes handled most of the intercepts. They were assigned some clerical helpers who did not need to do any independent work in the decipherment of messages. These helpers did not need to know Russian perfectly. They prepared counts of new messages, sorted the intercepts, after picking out the best copies they laid the others aside with a notation "duplicate". They were also entrusted with the simple task of entering the code values in the messages, using the already recovered codes and encipherments. The texts which they entered schematically were later corrected by the cryptanalyst when, due to garbles and errors in copying, the texts did not make sense. Those cryptanalysts who could do no independent work were also used as decoders.

When in the midst of the text place names occurred with special encipherment, those messages were passed to the group "Planquadrate" before they went to "Content Evaluation". This group deciphered these place names, which were enciphered by a special system, (they were generally sent in 5- or 6-digit groups) and entered the place names in place of the digit groups.

All messages from different cryptanalytic groups went to "Content Evaluation" after the complete text had been entered. "Content Evaluation" went over the text of each deciphered message carefully, noted all new information on its dislocation chart, made a radio situation report and forwarded this currently to the Air Force Command Staff. All newly noted troop units with their location or change of location were specially noted and reported to the Command Staff. "Content Evaluation" also kept a careful card file of all troop units, names of commanders, headquarters, types of planes, types of fuel, etc., which appeared in the messages and the Cryptanalytic Section often drew upon this when it needed precise data (names of troop units, types of planes, etc.) for the solution of a new code or for reading individual messages.

The current survey of the status of cryptanalysis as a whole and the practical work in all types of new cryptographic systems of the Air Force and the Army made it possible for me to evaluate the results of our cryptanalysis. It was clear that the work must be conducted from a different point of view in the Army and the Air Force. The movements of ground formations of the Army called for more time than did the movements of air units and this was taken into account in the decryption of the Army codes. The interval between the transmission of orders by radio and the execution of these orders within the air units was very short. For this reason the cryptanalytic work on the Air Force codes had to be done without loss of time.

In spite of the fact that it was not so vital in peace time that Air Force radiograms really be deciphered before the order for commitment (at maneuvers) was carried out, I insisted that the messages intercepted for practice purposes must be decrypted quickly, at least on the same day they were received. Every expert took an interest in seeing that the messages in his group were never left unworked till the following day. Only "New Decryption" was unable to adhere to the deadline, because solution of a new code called for several days of strenuous effort and especially for an adequate number of messages.

Radio Reconnaissance Service During the War.

Several hours before the German troops moved across the Polish border day and night service in three shifts was introduced at the Chiffrier-Stelle and the three outstations.

If the activity of the intercept service of the German Air Force before the war consisted of a number of separate tests, one might compare the work at the beginning of the war to a general test. The Chiffrier-Stelle with its cryptanalytic unit, evaluation unit and entire intelligence set-up was able to prove that after three years of existence it was equal to the task expected of it.

In spite of the Non-agression Pact between Germany and the Soviet Union, the intercept service against the Soviet Union was intensified. The Chiffrier-Stelle of the High Command of the Air Force and all its outstations were in a genuine state of alert. Every movement, every re-grouping of the Red Army as a whole was closely observed and reported to the Command Staff of the Air Force.

The cryptographic systems of the Red Army changed, to be sure, but in type and structure remained the same as before and could be handled by the cryptanalytic section without difficulty and without loss of time. From the intercepted and decryptqd traffic all troop assemblies and movements could be watched précisely. These observations were regarded with mixed feelings and with distrust by the Air Force Command Staff. Only one thing could be regarded as certain: one did not trust the other. And this mistrust became stronger when, after the conquest of Poland, the Red Army began to occupy the Polish territories promised to it.

Thanks to the currently read messages, the strength of the Russian troops that moved forward to the line of demarcation could be figured at over one million. Such strength of the Russian Army of Occupation in defeated Poland seemed a bit too high to the German Command Staff. The German Staffs followed somewhat nervously the movements of the Red Army, kept calling upon the intercept service for further reports and every-body waited tensely to see whether the Russian troops already in motion would cross the line of demarcation or would really stop there.

For their radio traffic the Russian troops were using some crypto-graphic systems and substitution tables which had already been solved by the cryptanalytic section of the Chiffrier-Stelle ObdL. The inter-cepted radiograms with 2-, 3- or even 4-digit groups could be solved up to 90%, deciphered and yielded perfect text. Here the decoding turned out to be well organized and well trained and in conjunction with evalua-tion supplied the Air Force Command Staff with valuable material. After all we were no longer concerned with maneuvers of the Red Army but with a very serious situation.

On this occasion the Cryptanalytic Section made an important discovery. Whereashitherto units of the Red Air Force had used only their Air Force code in their traffic, with the Polish campaign it was observed that commands from and to the Russian Air Force Staffs were also enciphered with the larger Army codes (OKK 2 = Commander Code Number 2). These messages, enciphered by the Commander Code were sent in 4-digit groups. Since the Cryptanalytic Section of the Chiffrier-Stelle ObdL had been interested in working promptly on the solution of the Commander Code for the sake of practice, these 4-digit intercepts could be decrypted currently. Since the text contained important orders and data of the Russian Air Force, special attention was paid to the interception of such messages.

With the ever increasing amount of intercepted traffic, the cryptanalytic work expanded more and more. It was necessary to engage more interpreters who knew Russian. This new personnel had to be introduced to the utterly new field of cryptanalysis. Only a few of the new interpreters proved useful for cryptanalysis, most of them, since they had already been initiated into the "Top Secret matters" had to be transferred to other sections ("Content Evaluation" or "Traffic Analysis") or be retained as helpers in the cryptologic units (as clerks or at best as decoders in the "Ausarbeitung").

There was a similar strengthening of the cryptanalytic and evaluation sections at the outstations. The new personnel was either introduced to the new work on the spot or was sent to the Chiffrier-Stelle for a four week training course. These new courses in cryptanalysis now had to be based on our new experience. It was no longer enough to be a good cryptanalyst acquainted with various types of systems, every expert had to have the following knowledge:

1. Special application of the Russian language in the cipher text.
2. Typical Russian military code book expressions and terms used in radio traffic.
3. Spelling mistakes which occurred frequently in enciphered Russian messages and which one absolutely had to reckon on.
4. The Russian habit of using different methods in their cipher service.
5. The carelessness and disregard for rules shown by Russian cipher personnel. These people frequently violated the rules and the German cryptanalysts were able to draw valuable conclusions as a result.
6. The mentality of the Russian signal personnel in general and in particular. The mistakes he was constantly making, thus partially compromising the secrecy of his own cryptographic service.

It was impossible to attack the Russian systems in the same way that we did those of the western countries. The Russian systems and their use were just as unpredictable as the Russians themselves. One could not solve Russian codes solely by the usual familiar principles of cryptanalysis, for they revealed their special character and had to be treated accordingly. In the three years before the war while the Russian signal service was being built up, we had time enough to become acquainted with everything and to accustom ourselves to these "usages". For this reason it was often possible during the German-Russian war to decrypt individual intercepts and to solve complicated codes with very little traffic.

The true general examination of the German cipher service began with the Finnish-Russian war. Here we had to do with serious military actions of the Red Army. And the Cryptanalytic Section of the German Air Force paid very special attention to these military actions.

Current reading of intercepted cipher messages continued without special difficulty. All messages intercepted could be decrypted and decoded perfectly, frequently much more rapidly than the Russians did it themselves. We could often notice this in the decrypted messages. And that was quite explicable. What did the cryptanalyst have to count on again and again in his work?

1. The Russian code clerk might make a mistake with his digits when enciphering.
2. The operator might make a mistake in transmitting the messages which consisted entirely of digit groups.
3. The interception might have been imperfect due to thunderstorms and a few digits or even some groups might have been copied incorrectly.

Consequently in addition to his purely cryptanalytic activity the decipherer had to deal with these errors in his work. The Russian cipher personnel which did its work in a routine manner could and would not concern itself with these errors into the bargain and in such cases was always requesting that the message be checked and resent. Meanwhile the cryptanalyst on the basis of his experience would have the defective message already decrypted. Furthermore it frequently happened that in

repeating the message the Russians would compose the text differently by another combination of digraphs and syllables and when the German cryptanalyst compared the repeated message with the first version he was able to identify new elements.

The decrypted traffic during the Finnish-Russian war was so fruitful and important that many new observations could be made. Among other things it could be determined that the supply of daily changing keys and also of new codes to the Russian mobile stations did not always function well. For this reason the Russian stations not infrequently sent important reports and orders, which otherwise would have been enciphered only in the Commander Code, enciphered by a primitive substitution table. Frequently this was done for want of time, but this always brought a stern reprimand from the control station.

The entire intercept service of the German Armed Forces was concentrated during the Finnish-Russian war primarily on the radio traffic of this campaign. Two-thirds of all our receivers were picking up everything that happened in this northern sector. Since there was plenty of traffic in this area and 90% of the messages could be deciphered, the Finnish Cryptologic Service received important reports in the speediest manner from the three German stations and could undertake effective countermeasures in good season.

The friendly close collaboration between the Finnish Cryptologic Agency and the Chi-Stelle of ObdL existed even before the Finnish-Russian war and was not merely maintained during the war but was even strengthened. The tough resistance of the Finns to the numerically far stronger enemy was due in large measure to the perfect functioning of the intercept service which promptly recognized every movement, every weakness of the enemy so that appropriate action could be taken.

Intercept Service in the German-Russian War.

A few hours before military action against the Soviet Union began, the fact that the action was about to begin was made known to the Chiffrier-Stelle ObdL in strict secrecy.

Despite the fact that in the three years of its activity the Entzifferung-Ost of the German Air Force had been functioning perfectly and really could face its future tasks calmly, a regular stage-fright came over all the cryptanalysts and especially myself as the leader and person solely responsible in this field. Everybody, clear up to the Air Force Command Staff, was aware that everything connected with the intercept service stands or falls along with the cryptanalytic work. What good would hundreds of intercepts be if they could not be decrypted, if they could only be used to clarify the networks. Just evaluating call signs and frequencies would not do the Air Force Command Staff much good. The "Content Evaluation" would be absolutely crippled if the intercepted enciphered messages remained undeciphered and so a certain nervous tension arose throughout the Chiffrier-Stelle of ObdL.

There was primarily one question which occupied my mind: Would the Russians stick to their former cryptographic methods or had they prepared special systems for the outbreak of the war which would now be put into effect and would set us back and upset our preparations and experience in the immediate future (which is the important time for the Command Staff)? It was clear to me that with the beginning of military action Russian traffic would show a change from the previous methods of using call signs and frequencies and of course a change of codes. The only question was whether the new codes would resemble the old ones in structure and type or whether they would be used in a manner hitherto unknown to us. There was no doubt as to our being able to solve the new codes but the Command Staff expected reports from us the very first day so as to learn immediately the early impressions of surprise and the countermeasures of the enemy and this might be delayed by many days if changes occurred.

The great value of the reports which the cryptologic service gave the Command Staff regularly before the war was fully recognized. For instance, the Air Force Command Staff received before the German-Russian war a dislocation chart, compiled by the cryptologic service on the basis

of its current intercepts which gave a clear picture of the state of Russian troops, their strength and character. From this dislocation chart it was also clear that there were great Russian troop concentrations on the German-Russian frontier in the area of Brest Litovsk. These important data were compiled from decrypted messages and could be regarded as 100% accurate.

German actions in this area began on the basis of this information. The Air Force Command Staff received from the Chiffrier-Stelle the exact strength of the Russian Air Force as well as the number of troops. The number of Russian airplanes of the first line reported by the Chi-Stelle turned out later to be correct.

It was clear that the staff expected further current reports from the Chiffrier-Stelle and that "Content Evaluation", which compiled its report from the decrypted messages, was looking hopefully to the Cryptanalytic Section.

In my section I made all possible preparation to achieve the quickest possible results as soon as intercepts came in. The best cryptanalysts were told to rest up so that they could be ready to pitch in and work for a long time when the first traffic arrived after the fighting started.

Our feverish expectation was relieved on the very first day of the fighting by a reassuring discovery. The first enciphered messages received after the fighting started could be solved quickly, to the surprise of all concerned.

It turned out that the Russian messages which were enciphered by the new codes remained the same as before in type and structure. Of course after a few days new observations indicated a fundamental change in the Russian radio and cipher service. Whereas hitherto the Russian Air Force had everywhere used one or at most two major codes, all the individual units now received codes of their own which they used to encipher messages exchanged over their radio networks. The results of this were as follows:

1. Because of the instability of the fronts and of the danger that the enemy might lay hands on the code, each troop unit was handed several rather simple codes which were to be short lived and could be replaced frequently by new codes.
2. The total number of intercepted messages was now divided between a number of codes which were in use simultaneously. All of which rendered the decryption of the various messages more difficult.
3. The frequent change of codes, though these were simple enough of themselves, called for the constant solving of new codes.
4. Due to the distribution of the intercepted messages over a number of codes which were in use only a short time the cryptanalysts were never able to work out the new codes to a point where the cipher texts could be read without gaps.

If the Russian Cryptographic Service had undertaken to carry through this dispersion tactic in a really exact fashion, the German Command Staff could not have counted on the swift fruitful decryption of the messages and the resulting daily air situation reports and radio situation reports.

But for some reason or other things were not carried out by the Russian cipher service as appearances first indicated. It is true that the separate units of the Russian Air Force continuedto use their own special codes for transmitting their messages but these codes remained in use for as long as four to six weeks and in the course of this time the messages could be worked out and the various codes brought close to completion.

On the average it is possible to count 20 to 30 different codes in use at the same time. Aside from these Air Force codes there were several "lone stalkers" and "one day flies" as they were called by the cryptanalysts of the Chi-Stelle, together with a multitude of substitution tables - with and without variants - in use. Further details will be mentioned later in the report.

Shortly after the beginning of the war with the Soviet Union the entire Chiffrier-Stelle ObdL moved its headquarters to East Prussia to be in the vicinity of the Air Force Command Staff. In order not to interrupt the current cryptanalytic effort and possibly miss changes in the Russian Cipher Service, during this move a number of good cryptanalysts were assigned to Outstation I (Königsberg), which was instructed to send its reports during this period to the Command Staffs. The outstations were merely to supply reports to the Air Fleets to which they had been assigned before the invasion. In addition the Chi-Stelle sent an advance unit (half its receivers, evaluators and cryptanalysts) to the new location and continued working with the other half in Berlin until the advance unit was able to start operating at the new location whereupon the remainder of the Chi-Stelle moved.

Since the Chi-Stelle of OKW and OKH were now separated geographically from that of ObdL and close collaboration and exchange of decrypted traffic could no longer take place regularly, I entered into negotiations with the Chief of OKW/Chi for the virtually crippled Cryptanalytic Unit of his agency. Since Chi/OKW was moving its entire outfit to East Prussia (Lötzen) and their cryptanalysts had no intercept stations of their own, they could not count on any traffic while they stayed in Berlin. On the other hand, the Cryptanalytic Group of OKW/Chi was well versed in the so-called additive enciphered code used by the Russians which was employed by the upper echelons and staff of the Red Army. Decrypted messages in this 5-digit code revealed that there were also air reports among them and that the traffic was of interest to the Chi-Stelle of the Air Force. Since we had no trained personnel of our own for this complicated system and since we could not, with our personnel, handle all the traffic in the 5-digit code, I suggested that the Cryptanalytic Group of OKW join the Chi-Stelle ObdL.

These negotiations led to a positive result. I succeeded in convincing the Chief of Chi/OKW that by geographically combining Cryptanalytic Sections of the two agencies we could do a complete job between us

on the additive enciphered code. The messages enciphered in this code were being intercepted by the operators of Chi-Stelle ObdL, all three outstations and the special station in Budapest and there were many of them. The traffic was very heavy (over 1,000 messages a day) and very important. It was decided that the Cryptanalytic Group of OKW should not be subordinated to the Chi-Stelle ObdL but would merely be assigned to it. It was to receive regularly from Chi/ObdL the 5-digit traffic. The Cryptanalytic Section of Chi-Stelle ObdL was to set up a special section for working on this additive enciphered code which would work in close contact with the group from OKW. The text of all enciphered 5-digit messages would go simultaneously to the "Evaluation Section" of the Chi-Stelle Obdl and to OKW in Berlin.

After this agreement the Cryptanalytic Group of OKW moved to East Prussia along with the Chi-Stelle ObdL (first to Nieden, than to Goldap). It worked independently and was paid and provided for (Betreut und Verflegt) by the Chi-Stelle ObdL.

Since I also set up in my section a group to work on the additive enciphered code and received from Chi/OKW the documents (code, difference catalogue) for decrypting the messages, I had to arrange things so that there would be no duplication of effort. Work on the 5-digit system (which will be discussed in Part II of this report) signified a great additional burden for my unit. But since the Air Force Command Staff was much interested in the content of these messages the work had to be done. For the purpose 20 helpers were procured who did not necessarily have to use the Russian language because they were concerned primarily with preliminary work on decipherment of the 5-digit system.

All 5-digit messages that were intercepted and reached the Chi-Stelle ObdL were sorted by these 20 men, working in three shifts, in the method prescribed. Messages enciphered by various additive tables, characterized by indicator groups, belonged to one series or another. When there were more than 5 messages belonging to the one series, we considered this one capable of decryption and work on it began.

In order to get together such a series it was necessary that all 5-digit traffic be sorted carefully and that the interception of these messages be guided. All 5-digit traffic was grouped by the several series and whenever a series attained a depth of five, i.e., had 5-messages, it was worked on by the cryptanalyst.

To facilitate the complicated task of the cryptanalysts, the messages of the same series were copied on teleprinter tape and pasted together one beneath the other. In this way the cryptanalyst got a better survey of the messages of a series and could also more readily carry on his work with a difference catalogue to determine the key numbers. Nevertheless a good cryptanalyst who had become accustomed to the procedure could only work on two or three series a day at most. Such series however as could be worked numbered some 30 to 40 a day. Some series embraced as many as 10 to 15 messages so that the number of 5-digit messages to be worked on ran as high as 300 in a day. It must also be noted that these 5-digit messages often were from 100 to 200 groups in length and that each group usually represented words or even sentences.

The work was somewhat facilitated when the additive enciphered code was captured so that we could simply employ our special method of stripping the additive. It was noteworthy that the Russians did not replace this code by another after it was captured. We assumed that the Russians either had not immediately noticed the capture of this important code or else that the unit which had been unable to destroy it in time had failed to report this to higher authority for fear of being punished and that finally the Russian Cryptographic Units might be so firmly convinced that this complicated system could not be solved that they did not introduce the new code for a month.

The decrypted messages in this code contained extraordinarily important reports and orders sent from one staff to another. They contained complete lists of losses of men and material, the combination of several scattered and virtually annihilated divisions. In them was reported the status of the troop units, supply, regroupings of units of all branches, and impending actions.

By means of these perfectly decrypted messages the German Command Staff of the Army and the Air Force had the precise picture and could plan their own measures in reliance thereon. Unfortunately the 5-digit traffic was so extensive that the few experts who were able to deal with the code could not possibly decrypt everything.

It had been a mistake from the beginning that the German Armed Forces did not combine and centralize the three cryptologic agencies of OKW, OKH and ObdL. It is true, Chi/OKW tried to accomplish this before the war but ObdL and OKH asserted their independence and each agency expanded its layout more and more and became larger and larger from year to year. Nevertheless the three agencies lacked really good experts both in cryptanalysis and in evaluation although all of them employed a terrific number of people. It is worthwhile to take a look here at the organization of the three cryptanalytic agencies of OKW, OKH and ObdL and the number of persons employed in the agencies and their subdivisions (or outstations) so as to get an idea of the sense of the whole arrangement.

Each (Central Cryptologic Agency (OKH and ObdL)) employed during the German-Russian war:

1. 100 to 150 cryptanalysts (including helpers).
2. 40 to 50 content evaluators.
3. 20 to 30 traffic analysts.
4. 45 to 60 operators (15 to 20 receivers).

To these must be added: personnel for the administrative office of the agency, for the teletype unit, the clothing supply, paymaster, housekeeping and telephone exchange.

Each of the three outstations of each of the agencies, i.e., 6 outstations, employed in addition:

1. 50 to 60 cryptanalysts (including helpers).
2. 15 to 20 content evaluators.
3. 10 to 15 traffic analysts.
4. 45 to 60 operators (15 to 20 receivers).

and the necessary administrative personnel, teleprinter personnel, etc.

Each outstation also had its subordinate stations which were equipped with only a few receivers and manned by operators and a few cryptanalysts and evaluators.

Summing up, all the agencies and outstations of OKH and ObdL plus part of OKW employed during the war:

1. Cryptanalysts 550 to 650 men (10% really good).
2. Content evaluators 200 to 230 men (10% really good).
3. Traffic analysts 120 to 140 (10% really good).
4. Operators 370 to 480.
5. Receivers 150 to 160.

and about 120 to 150 persons in administration, teleprinter, clothing, paymaster, telephone and housekeeping.

It is interesting to note that there were never more than 10% really good experts at any agency, especially in cryptanalysis, these being the people one must rely upon to get this special work done. These 10% were too few for the amount of work involved, as each agency could confirm, and the Heads of the Cryptologic Sections were always beating their brains out trying to find the best way to handle all this traffic with the few available specialists. It should also be noted that the above number of cryptanalysts was divided into three shifts so that in reality you could count on only one-third. For this reason it was impossible to divide the best cryptanalysts into shifts along with all the rest, instead they had to be kept available at all times. In the course of time these lone specialists were overworked and, as the war went on, could no longer do the best they were capable of.

If there had been a single Cryptologic Agency from the very beginning, the main unit and the three outstations for handling all traffic of the Red Army might have been as follows:

1.	Cryptanalysts	300 to 350
2.	Content evaluators	100 to 120
3.	Traffic analysts	60 to 70
4.	Operators	300 to 360
5.	Receivers	100 to 120

with some 80 persons for administration, teleprinter, clothing, telephone, etc. Aside from the fact that this centralization would have saved about half the personnel, the quality would have been raised some 20 to 25 percent. The best talents could have been employed where they were most urgently needed. However, this centralization was not put through and the few good workers available at the many stations of the Army and Air Force could not handle all the work and do it well.

In order to help themselves out, the Heads of the Cryptanalytic Sections of OKW, OKH and ObdL attempted to work together on their own initiative. When I found out that the 5-digit traffic could not be handled in toto by my men and by the cryptanalysts of the OKW group working with us and found that Chi/OKH was working on the same traffic, deciphering the same messages and not able to handle all its material, I went to the Chief of Chi/OKH with whom I was well acquainted. I proposed close collaboration of the three cryptanalytic groups in order to handle the 5-digit material on a mutual basis and to cut out duplication of effort. In order to accomplish this it was necessary to lay a direct telephone line between the Cryptanalytic Section of ObdL and that of OKH. Over this direct wire the units of the two stations had to announce the series of 5-digit messages they were attacking so that the same series would not be worked on twice but some other nearby series would be selected. For instance if Chi/OKH were to announce work on several series, it would get from Chi/ObdL all messages of the same day in these series by courier and this would facilitate the work. Chi/OKH did the same with messages available at its stations in the series selected by the Air Force.

This proposal was accepted. A direct line was laid at once and within a short time duplicate work on the various series could be stopped and more series could be decrypted.

The Command Staffs of the Army and the Air Force currently received extensive reports drawn from this traffic.

Parallel to the fruitful but difficult cryptanalytic work on the 5-digit code difficulties increased in the decryption of the 3- and 4-digit codes and the substitution tables.

The Russian Air Force consisted of many Air Armies - V.A. = Vozdushnaya Armiya (Air Army) to which were assigned ground organizations such as the RAB (Rajonnaya Avia Basa = District Air Base), to which in turn were assigned the BAO (Battalion Aerodromnogo Obsluzhivanya = battalion for air field maintenance). These units had their own radio stations to which were attached cryptographic personnel which enciphered the messages with the assigned code..

Thus in the various networks of the Air Force Signal Service different codes were assigned to each V.A., to each individual RAB and BAO. To each Air Army were assigned several RAB's and to each RAB several BAO's. The intake of 2-, 3- and 4-digit messages ran between 600 and 1000 a day. In order to ascertain the particular code of the above-mentioned units to which these messages belonged we had to have a reorganization. Just how was the cryptanalytic work of the Air Force organized?

1. Since each V.A., RAB and BAO had its own code for the encipherment of radiograms, some 30 to 40 codes were regularly in use daily.

2. The intercepted messages (excluding 5-digit messages) averaging between 600 and 1000 a day were distributed among these 30 to 40 codes and substitution tables and had to be recognized and interpreted.

3. New codes were constantly appearing which had to be solved.

4. In the course of time the new Air Force codes were better constructed and more complicated, the superencipherments were refined, so that our survey of the situation became less and less complete.

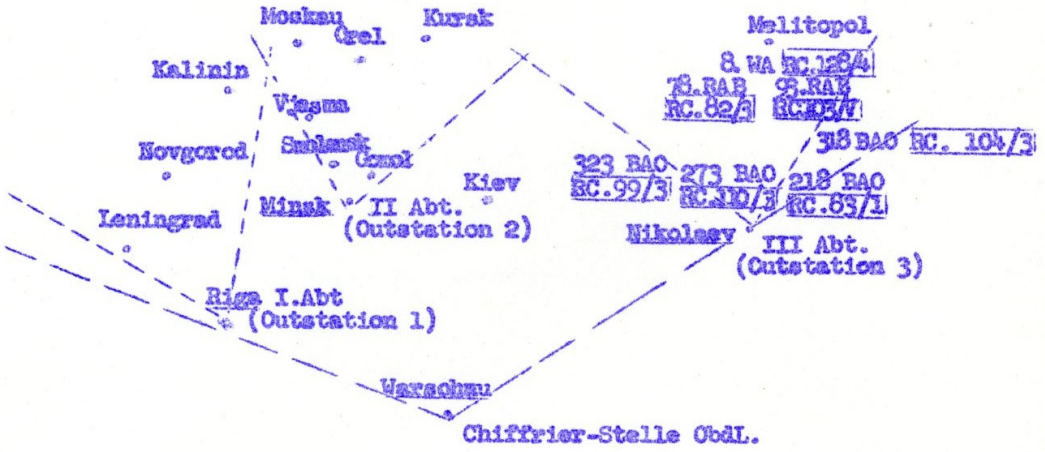
5. The new systems of encipherment not only made it possible to change the keys frequently during the day but even to do so within a long message and also made it possible to encipher faster and more securely although decipherment was not so easy.

Russian signals communication developed more and more during the war. The great distances and the situation on the different fronts called for constant contact of the several units with one another. Codes and superencipherments which had fallen into the enemy's hands had to be replaced frequently by new codes. This constant procession of new codes increased the watchfulness of the German cryptanalysts and also called on them for increased effort. The Chiffrier-Stelle ObdL had to increase its personnel and had to provide for an increase at the three outstations in order to master the work.

In order to relieve the outstations, which did not have enough good cryptanalysts, I ordered that traffic which had to be newly decrypted at the three outstations should be collected according to links (nets).

The outstations were free to choose one or two systems out of the total traffic to work on locally. All the other undeciphered traffic had to be sent at once to Chi-Stelle ObdL. The Cryptanalytic Group at the Chi-Stelle specialized principally in new decryption, this group was increased and provided the outstations with newly decrypted material so that they could decode their own intercepts.

Aside from these working materials all the cryptanalytic groups of the agency and the three outstations, like Chi/OKW, Chi/OKH and the two stations in Finland and Hungary, received a sort of dislocation chart (survey chart) showing the state of decryption. On this chart were entered all Russian Air Units identified by the intercept service. Alongside the designation of the unit, e.g., 8.VA (8th Air Army) or 78 RAB or 364 BAO, were entered also the codes (number of the code) used by the units. These survey charts were corrected twice a month by the Cryptanalytic Section of the Chi-Stelle ObdL and were sent out regularly. Every outstation was thus able to check and see which unit of the Russian Air Force and which associated codes were in its area and what cryptographic systems it was supposed to be working on. Only units lying at the intersection of the areas of two outstations were worked by both outstations.



Note: The numbers of the VA, RAB and BAO as well as the numbers of the codes, used in this example have been chosen arbitrarily. The same is true of the locations.

success and fully justified the existence of the Intercept Service.

In the survey chart shown here, we have given as an example only the 8th Air Army with its RAB's and BAO's in the Southern Sector. During the war one could count 20 to 30 different Air Armies distributed over the three sectors. Their headquarters and codes changed constantly. Their precise location was obtained from decrypted messages and by direction finding. The term RC 128/4 signified the serial number of the solved Russian codes, in this case the 128th solved Russian code which was sent in 4-digit groups (with a 4-digit encipherment). The adjacent Air Armies maintained radio connection with one another whereas the RAB's and BAO's were only permitted to maintain radio contact within the area of their own Air Army.

All solved and well worked out codes which appeared in the intercept area of Outstation North (in Riga) were sent regularly along with the survey chart to the liaison officer of the Chiffrier-Stelle ObdL in Helsinki for delivery to the Finnish Cryptologic Service. The same thing happened in the intercept area of Outstation South (in Nikolaev). All codes and survey charts which appeared there were sent to the Hungarian Cryptologic Service in Budapest.

The Chiffrier-Stelle ObdL had therefore not merely the task of working for its own Air Force Command Staff but had to see to it as the court of final appeal (especially in cryptanalysis) for the entire intercept service in the East, that all stations of the Air Force received regularly equally complete cipher materials and had to work in close contact and maintain an exchange of material with the Finnish and Hungarian Service.

For these purposes it was necessary to provide suitable communication facilities at all these stations which was done throughout the war by teleprinter and telephone lines. Since during the war the distances of outstations from the Chi-Stelle ObdL became ever greater (Riga, Helsinki, Smolensk, Budapest, Caucasus), newly solved codes and keys often had to be transmitted by radio. Such messages were then enciphered by the German machine keys.

I should like to introduce here a few striking examples which, because of fast perfect work on the part of the Cryptanalytic Section, resulted in success and fully justified the existence of the Intercept Service.

From these few examples it will be clear that the enemy had to resort to primitive means of encipherment in order to transmit information to its destination.

In the first months of the war one message among others was intercepted and decrypted which, strange to relate, was enciphered by a simple substitution table. Since the message was enciphered solely in letter text it could be solved 100% very quickly.

From this message it appeared that a Russian bomber formation of 40 bombers (TB-3) was starting at such and such a time from a precisely designated airfield, and would fly a course indicated by coordinates in order to attack and annihilate the German troop concentration at such and such a point. This radiogram which was deciphered very quickly, went with its precise data without delay through Content Evaluation to the Command Staff and to the Air Fleet in the area concerned. The Air Fleet was able to transmit in time to a group of MÖlders (pursuit squadron) the order to start. 60 pursuit planes flew to meet the Russian bombers and destroyed them to the last plane.

In another case the destruction of a convoy near Murmansk was involved. This time during the course of several days messages were intercepted and decrypted in which a convoy of some 40 vessels was reported which was on its way to Murmansk. In these messages the position of the convoy was given repeatedly. All the messages were enciphered with a simple substitution table and could be deciphered in full very quickly. The Air Fleet in the North could be alerted in time. A large number of bombers was ready to start. Then when additional decrypted messages announced the approach of the convoy to Murmansk the German bombers were ordered to start. The exact position of the attack was known. Here again the attack came as a surprise and destroyed nearly all the ships.

From these two examples one might assume that the enemy did not count on the possibility that the German Intercept Service could decrypt the enciphered messages in time. But why this important message was enciphered in such primitive fashion is hard to explain.

There was neither lack of time nor lack of better codes or ciphers. All Russian stations were stricily forbidden to encipher important messages with the substitution table but nevertheless they did it and kept on doing it during the entire war.

In another case, at a later point of time, the enemy did reckon on the existence of a German Cryptanalytic Unit. This was an emergency case.

A Russian unit, which was in flight was stuck on the shore at a bend in the Don and radioed an alarm enciphered by a simple Caesar to its superior unit. It said it was on the right bank of the Don in area such and such with 90 motor vehicles (armoured reconnaissance cars, radio cars and trucks) and with a crew of so and so many men, in flight from the ever oncoming enemy. It requested that a troop of engineers be sent as quickly as possible to construct a bridge over the river.

Immediately afterward the station called sent its answer. In the message the commander, who was in a desperate predicament, was reproached for having frivolously sent his report enciphered in such a simple fashion. The message, which was enciphered in a code, went on to say that the enemy would send its Air Force and destroy them all before help could arrive.

A lively exchange of telegrams between the two units ensued. The unit on the Don continued to encipher its messages with the substitution table. It reported that it could not decipher the messages received because it did not have this code. It could only encipher and decipher with this table.

Meanwhile this call for help and the ensuing conversation between the two stations had been decrypted perfectly by the Chi-Stelle ObdL. It was able to read the messages enciphered by the substitution table as well as those in the Air Force code. The report with the exact data went immediately to Air Fleet South. At the same time the operators were told to watch this traffic closely so as to get any further details. What was anticipated in the dispatches actually took place. As could be learned from an air photograph the whole group with its 90 vehicles was destroyed completely by the German Air Force.

From this example it is clear that the unit which had gotten into trouble had no other code on its flight save the simple substitution key and could only encipher its messages in this primitive fashion. It hoped perhaps that help would come before the enemy deciphered the message.

Such cases in this very mobile recent war occurred rather often. The danger of losing to the enemy comprehensive cryptographic systems with their complicated encipherments forced the top unit, (the Cryptologic Agency in Moscow) to give those units committed to battle and exposed to such danger, simple, frequently changing substitution tables and small codes for the encipherment of their messages. If these substitution tables with variants had been properly and conscientiously employed, then the German cryptanalysts would have needed much more time to decrypt the messages. But for the most part, due to the primitive character of the simple radio personnel and to no less a degree to reasons of convenience, this possibility was not utilized to the full.

Such success stories were not rare throughout the war and the Cryptanalytic Unit of the German Air Force could well be content with its work right down to the end of the war. It worked fast, often deciphered the intercept quicker than the Russians did themselves, was able to follow the development of the Russian Cryptographic Service, precisely and currently and was able to keep step with it all the while.

During the war various captured codes and ciphers of the Russian Air Force fell into German hands, these captured codes were passed immediately to the Chiffrier-Stelle ObdL and I was able to compare them with the codes solved and compiled in the Cryptanalytic Section. Again and again it turned out that the codes and system tables compiled in the German units were essentially correct. The difference was that the original codes of the Russians were usually in book form and that the leaves had to be turned when using them. In contrast the codes recovered and reduced to basic form in the Chi-Stelle ObdL were entered on a single sheet so they could be used more easily.

This sheet was divided into 10 long columns which corresponded to the rows of the original code page. (See Appendices II and III in Part II of this Report). Thus we had the entire code before our eyes which

essentially facilitated decoding and filling in gaps in the code.

Since in each group the same workers were assigned to particular types of codes, in order that they might be able to pick out, from the mass of traffic those enciphered messages which were familiar to them, the individual workers could not be acquainted with the other types of codes. For this reason I instituted a monthly exchange of ideas and experiences in the Cryptanalytic Section. The analysts gathered new inspiration from one another and expanded their knowledge of the subject as a whole. The codes deciphered by the Army were also shown and explained in order that they might become acquainted with these systems too.

When the Chiffrier-Stelle ObdL (East) was transferred to Russia (to the vicinity of the Air Force Command Staff) the Cryptanalytic Group of Chi/OKW, which had been working in close collaboration with the Air Unit all the while, could not be transferred too.

Here another factor played an important part. The excellent collaboration and the good results of the mutual cryptanalytic effort of the two agencies gave the Cryptologic Agency of OKH no peace. The rivalry did not last long. Higher authority made it clear that the two Cryptologic Agencies OKW and OKH fitted together better in the field of Army cryptanalysis and the Air Force renounced the collaboration of the OKW group which was then attached to the Chi-Stelle OKH (Lötzen, later Vinnitsa) and transferred its entire unit to Russia. In the end it was immaterial which unit the OKW group worked with and which unit had the advantage of its well trained people. The only interesting thing was that at the beginning of the German-Russian war the Cryptologic Agency of OKH displayed no interest in the Cryptanalytic Group of OKW. Not until the successes of the Chi-Stelle ObdL in the encipherment of the 5-digit additive enciphered code became more pronounced, did it pay any attention to the assisting talent of OKW and begin to fight for them. Later it turned out that the Chi-Stelle OKH was not gunning for the cryptanalysts of OKW but was only trying to separate the two cryptanalytic groups which were collaborating so well. Once the Cryptanalytic Group of OKW had been separated from ObdL and was installed with its former rivals of OKH, the Chi-Stelle OKH took no further interest in the Cryptanalytic Group of OKW and did not allow it to do any particular work.

Since the 5-digit systems (additive) were 80 percent an Army matter and the Cryptanalytic Group of the Air Force had enough to do with its own Air Force systems, interception of the 5-digit messages was discontinued save for a few which were needed to check on the networks.

After the Chiffrier-Stelle ObdL (East) moved to Russia, close collaboration with the Cryptologic Agencies of OKW and OKH was interrupted for a considerable period of time. Only after some time, when the Chi-Stelle OKH moved to Russia (Vinnitsa) was it possible for occasional personal contacts and discussions between the two cryptanalytic groups to be resumed. But the good contact and good collaboration that had existed existed no longer.

During the further course of the war with the Soviet Union, the systems and types of Russian cryptographic systems improved more and more. The codes and the manner of encipherment were worked out so well that if the messages had been enciphered in precise accordance with regulations, only a portion of the intercepts could have been deciphered. The Russian code clerks, however, did not follow the rules very strictly and the German cryptanalysts were able to decrypt all the codes and tables which appeared down to the end of the war.

With the 5-digit systems it was a different story. Each encipherment table (additive table) was used only once, i.e., each message was enciphered with a new table so that it was no longer possible to decipher the 5-digit messages. Only very rarely did cases occur where two, or at most three messages were enciphered with one and the same table. Such cases only occurred when the supply of blocks was not effected promptly but that happened only rarely.

The army regarded these new facts with regret but had to make the best of it and worked principally on the cryptographic systems of the Border Guard (NKVD) which sent plenty of messages that could be decrypted.

The Cryptanalytic Section of the Air Force was able at all times to decipher up to 70% of all intercepted messages of the Russian Air Force. Codes were changed frequently, many new types were introduced, but essentially the codes remained similar in their structure. The decrypted

traffic continued to be extensive and very important for its content. The German Air Force Command Staff was not able to do much with it, however, because it did not have means for carrying out countermeasures. The Command Staff noted all these reports with regret, continued to enter them very carefully in the situation charts, but generally this entry was the end of the story.

All the intentions and preparations of the enemy down to the last great offensive in the East could be recognized and notice was given promptly on the basis of decrypted traffic. The tragedy of the collapse of the German Front on the East and the Russian break-through, encirclements and advances toward Berlin were known to the cryptanalytic personnel before they actually took place. It is easy to understand that the spirit of the cryptanalysts and the evaluators in particular who thus learned the whole truth, was not of the best. All their work seemed to be in vain and yet they all sat there day and night over their messages and decrypted them just as intently as they had done in the days of the great successful encirclement battles in Russia. They remained at their posts till the very end feeling certain that by their effort they could help their comrades at the Front.

I was often reproached by higher-ups who said that the morale of my cryptanalysts left much to be desired, that their conversations with one another and their opinions were dangerous, and orders were given to have the personnel enlightened by political lectures. These orientation lectures, however, contrasted sharply with the text of the decrypted messages which were known to all the cryptanalysts.

As proof of the unsurpassed accomplishment of "Entzifferung-Ost" of the German Air Force will serve the 946 different Russian codes which were solved satisfactorily after the beginning of the German-Russian war. In this number are not included small codes which were used only a few days or the substitution tables, with and without variants, which numbered over 400. All these codes and tables were collected by me as "Archive" for the Chiffrier-Stelle ObdL. They were destroyed in the Wildpark (Potsdam) shortly before the collapse.

The working copies of the codes which were constantly in use were (supposedly ?) put in a safe place at the time of the capitulation by the officers of the air signals regiment. Whether these working codes were destroyed or fell into the hands of the enemy is not known to me. In the final days of the war, safeguarding the secrecy of "Top Secret" material was no longer taken very seriously.

Irrespective of how the Second World War ended, the Entzifferung-Ost and the Chiffrier-Stelle ObdL can without hesitation boast of its excellent and successful activity from the time it was established down to the end of the war. It gathered a great deal of useful experience and made some interesting discoveries in the field of the intercept service which may be of value even in the future for those who concern themselves or should concern themselves with this subject. The material dealing with this special science is inexhaustible. This work which was extraordinary and unique was carried on in strictest secrecy and was known and available only to those with the highest security clearances.

END OF PART I

Part II

General survey of various types of ciphers used in the traffic of the Red Army and their structure.

The Russian Cryptographic Service really introduced two basic forms of cryptographic systems for the radio traffic of the Air Force. These were "Cäsaren-Tafel" and "Satzbücher" [substitution tables and codes]. These two types were set up in all possible variations and forms. In appearance they were always different, the methods of encipherment were varied and complicated but nevertheless were simple in application. These two types of cryptographic systems were continued in use by the Russians during the whole of World War II.

Cäsaren-Tafel

The simple substitution tables were great favorites with the Russians. Really they were only supposed to be used for procedure messages of the radio stations but were often used in transmitting important dispatches.

The structure of these tables was generally limited to a 10 x 10 square. The variations were numerous and the types of encipherment manifold. Only a few were completely different in type and structure.

Form 1: Table without variants.

The letters of the Russian alphabet were entered only once in the table and in alphabetic sequence. Aside from the letters the table contained marks of punctuation, numbers and at most a few operational signals.

Form 2: Table with variants.

All the letters of the Russian alphabet appeared more than once in the table. The most frequent letters occurred more frequently than the rarer ones. In this table numbers, marks of punctuation and occasionally operational signals were found.

Form 3: Expanded tables.

Aside from the letters with variants, words appear in this table (e.g., of, on, in, too, etc.) and numbers and marks of punctuation are assigned variants.

Structure, use and solution of the "PP"

Form 1

	8	4	9	2	6	7	Ø	1	3	5
7	А	К	Ф	Ø	,					
1	Б	Л	Х	1	.					
9	В	М	Ц	2	-					
2	Г	Н	Ч	3	:					
8	Д	О	Ш	4	'					
5	Е	П	Щ	5	?					
Ø	Ж	Р	Ы	6	"					
3	З	С	Ь	7	(					
6	И	Т	Ю	8	)					
4	Й	У	Я	9	!					

This simple basic table contained only letters, marks of punctuation and digits. Each element was expressed by 2-digits. The horizontal and vertical coordinates (encipherment sequence) were changed regularly (daily). They must be known to the sender and receiver. In this way the single elements of this table were always expressed by dinomes, e.g. A=78, E=58, M=94, T=64, H=19, etc. The enciphered letters were sent in 2-digit groups in the message. The radiogram contained, in addition to these 2-digit groups, call sign and an indicator showing the number of 2-digit groups contained in the cipher text.

Form 2

	3	6	9	2	Ø	5	7	1	9	4
21	С	Ø	П	Е	Б	Е	Т	У	А	С
97	1	Г	В	Р	.	Ш	'	Г	И	Я
52	С	2	А	3	З	Б	Е	Р	Ь	.
33	З	Ф	Р	Е	А	Д	И	(	)	-
54	Т	О	В	Т	Ы	К	Т	Ч	Р	Л
89	Ж	Х	Е	О	4	Н	С	Е	И	М
76	Р	А	С	Е	В	5	А	Н	,	'
12	К	О	Щ	Я	Д	О	6	Ы	И	Л
47	Ь	Д	В	Е	И	М	О	7	-	Н
Ø5	И	Ц	К	Й	О	В	К	Ю	8	9

These two forms were used in the same manner as Form 1. The three types of encipherment could be used for any one of the three forms. In rare cases the Russians also used mixed encipherment, e.g.,

horizontal = digits

vertical = letters

But in most cases the Russiansused only three types of encipherment mentioned here. The table with variants (Form 2) was so constructed that the most common letters of the Russian alphabet occurred per-centually more often than the rare ones. Form 3 was an expanded table which contained a few important, often used syllables as well. The cipher clerk had a chance to disguise the frequency of the individual

Form 3

	83	64	29	Ø1	38	65	Ø9	32	4Ø	15
66	Ø	Г	Ь	Ш	Е	Щ	Р	Ы	8	Е
13	С	Ч	П	А	О	Ю	М	НА	НЕ	НО
48	Ж	І	В	Я	И	В	ПРО	7	Р	Н
76	Ц	М	Е	Д	9	П	З	Е	ДО	И
23	Б	К	2	И	В	ПО	6	О	Н	Ф
77	О	Х	Ж	(	А	)	О	НАЧ	В	Р
ØØ	Е	Л	,	З	-	5	Б	КОМ	ИЗ	У
72	Р	.	-	К	Д	О	ПРИ	ОТ	М	Ь
54	Н	А	"	Ч	ПО	ЗА	Е	ОВ	А	НО
63	.	О	Л	И	С	К	ВО	Т	Н	К

letters by making the proper choice. The Russians did not fully utilize this advantage of the tables with variants. For convenience they usually picked the same letters from the table and thus could not avoid revealing the frequency of the letters which occurred often.

Form 3, with its 4-digit encipherment, could give the impression of a code and deceive the cryptanalyst. Of course it would not escape a trained eye that the first and second dinome had only been selected from the same groups of 10.

These three basic forms could be enciphered in different fashions:

Variant 1: Simple encipherment without variants, e.g.

vertical: 7 1 9 2 8 5 0 3 6 4

horizontal: 8 4 9 2 6 7 0 1 3 5

Variant 2: 3-digit encipherment, e.g.:

vertical: 21 97 52 33 54 89 76 12 47 05

horizontal: 3 6 9 2 0 5 7 1 9 4

Variant 3: 4-digit encipherment, e.g.:

vertical: 66 13 48 76 23 77 00 72 54 63

horizontal: 83 64 29 01 38 65 08 32 40 15

All these variants contain therefore only ten different encipherment numbers as was brought about by the 10 x 10 table. They could be applied at random and to any substitution table. Since they were limited to just ten different monomes or dinomes, the radiograms could be recognized as in a substitution key even when sent in 3- or 4-digit groups.

Solution of the substitution tables.

Solution of the substitution tables and their encipherment proceeded as follows: all messages having the same digit groups in their cipher text were subjected to a count using a 10 x 10 table in order to get the frequency of the individual digit groups.

Message (enciphered text)

to KFB2 - from LMC1 Time 14.35, Date: 6.7.1937, 153 groups

15 82 13 89 43 65 82 52 95 88 25 75 45 43 93 15
22 35 22 42 55 22 15 15 45 32 73 05 55 82 65 03
25 62 45 15 62 75 15 95 63 75 45 65 95 42 55 93
25 45 05 65 75 45 98 85 22 35 45 05 65 82 13 22
75 22 02 42 45 15 88 15 82 53 45 72 95 05 03 15
28 25 75 82 32 45 35 52 22 75 22 12 95 75 22 85
62 32 52 55 62 02 62 42 22 75 22 32 15 62 85 45
55 45 35 22 15 85 62 05 97 87 82 83 65 45 35 82
43 62 15 82 35 62 88 85 45 43 88 52 75 65 12 88
35 22 55 03 15 62 85 45 32 etc.

These 153 2-digit groups are subjected to a count, (see 10 x 10 table below). The frequency of the individual groups reveals clearly that we have to do here with a letter text and that each two digit group must represent a letter, a digit or a mark of punctuation.

Count

	0	1	2	3	4	5	6	7	8	9
0			З	Б		С				
1			Г	Ч		М				
2			Е	Ш		П				
3			В	Ц		Н				
4			Д	Щ		О				
5			З	Х		Л				
6			И	Ъ		Т				
7			Ж	Ы		Р				
8			А	Ф		К			⊙	
9			Й	Я		У				

The differing frequencies of the individual groups make it clear that in the count two columns have the heaviest score. The third column shows relatively few 2-digit groups, the 4th and 5th show only sporadic groups. Keeping this count in mind we study the cipher text with an eye to the individual groups. The most frequent groups are marked and other striking characteristics are also indicated by special markings.

At first glance the group 88 attracts attention since only one cell in the column is scored and since it occurs once only at the beginning and at the end of the message and once in the middle while the intervals are regular.

If it were a rare letter it would not occur this way in the text. if it were a frequent letter, then, since it does occur 6 times in the cipher text, the group would inevitably be distributed regularly throughout the message as is the case for 45 and 22. Consequently it can only be a mark of punctuation and only a "period" because it appears primarily at the beginning and end of the message and consequently sets off the address and the signature.

Moreover the two groups 97 and 87, which stand next to one another and occur only once, cannot be either letters or marks of punctuation. These two groups are in a special column and may perhaps be digits.

Columns two and five, judging by their frequency can only be columns of letters. Regarding Column 3 we cannot say very much for the present because the frequency of the individual group is close to a minimum.

The new Russian alphabet has 30 letters. Judging by the count, the letters have been entered in three columns: two, three and five. The other two columns may contain digits and marks of punctuation.

Groups 45 and 22 occur most frequently in the count. In the frequency curve of the Russian alphabet the letter O occupies the first place, followed by V, E, R, I, S, etc., hence primarily vowels.

(These frequencies have not been taken from ordinary text but from military text).

The vowels are distributed evenly throughout the entire text. Group 45 is so distributed. Group 22 is often found next to 75 which also occurs frequently in the count. In each case the group before and after 22 is different. These groups occur rather rarely in the count. Hence we can assume with certainty that group 22 is also a vowel because it is rare that several consonants occur one after the other in the Russian language.

These two groups 45 and 22, which have been assumed to be vowels, are underscored in red in the message. After we have assumed that 88 is "period," we find nine 9-digit groups toward the end of the message which stand after 88, i.e., after a period. So we can assume with certainty, since all these nine groups show a fair degree of frequency, that we have here a name as signature. The group 45 stands in the next to the last position ahead of another, 32, which occurs a few times in the message. Many Russian names end in "OV" [OV]*. The group 45 has been assumed to be a vowel and this would be

*Translator's note: transliterated into English is OV.

confirmed if we assume it to be "O". Then the group 32 might be W [V]. Since group 22 has been regarded as another vowel, it might be either E or I.

In the 23rd and 24th positions of the message two identical groups come together - 15. This occurs in the letter column of the count and is frequent. Therefore it can only be a letter which occurs as a doublet. In Russian N or M are most often found as a doublet. If this could be an N and if 22 were an E and 45 an O as we have assumed, we should have a four letter sequence - ENNO, which sounds like a possible syllable. Before this assumed syllable the group 22 occurs twice, once following 15. Replacing these groups by the letters assumed, the passage appears as follows:
N E . E . . E N N O . . . The word is "NEMEDLENNO" and means "at once."

We enter these interpreted letters in the corresponding cells of our count and also above the groups in the message.

Before our word "NEMEDLENNO" stand five groups, one of which 45 = O is already known while another is 75 which occurs very often, including an occurrence together with 22, i.e., with E. Then come two letters which occur isolated. Since ahead of these five groups we again have group 88 (period) setting off the address, we know that the message text begins after the group 88. In connection with the word "NEMEDLENNO" the Russian word "Proshu" i.e., "please" is frequently found in Russian. Since the group 45 is known to be O and 45 stands in the third position we can assume with virtual certainty that this assumption was correct. Therefore we have: Proshu nemedlenno please immediately ..... .

Now we can enter four new letters in the table and in the message all identical groups have the interpreted letters entered above them. We then find a few places which suggest further guesses and interpretations.

We have already assumed that the beginning and end of the message may be an address and the signature. The address begins with the letter N, then come two groups and the period. Then Sh, three groups, then A and another period. The group 82 occurs in both series of groups and according to the count is a very frequent letter, after N and Sh with another letter it might be a vowel. O and E have already been assigned. Only A and I are left.

On our first attempt to fill out the gaps with A we get the following: N A . period Sh . A . U period . Consequently the address could only be Nach . Shtaba . (Ch as one letter), i.e., Chief of Staff. "Nach" is actually an abbreviation of "Nachalnik" (Chief). The Russians often used such abbreviations of ranks, primarily in radiograms.

After this interpretation we can enter new letters in the table and in the text which suggest further combinations.

The group 65 occurs fairly often in the count. After all the letters have been entered which have been interpreted thus far and after we have looked through the already deciphered portion of the message, we can fill in gaps here and there with missing letters.

For instance, in the middle of the message NA (= on the) pravom (right) bere . u (can only be beregu = bank) then comes RE.. which can only be reki (river). Summing up: Na pravom beregu reki (on the right bank of the river).

These newly interpreted letters must also be entered in the table and in the message. Completion of the text is not difficult now. The sense in combination with the still missing letters soon gives us the entire text.

For this example of decipherment of a message we have taken an ordinary easy text. We have tried here by means of this text to show a simple and logical trend of thought such as will be used in connection with other more complicated types. It is absolutely essential that one should not only be a master of the Russian language and be acquainted with the frequencies and with the combinations of the individual letters, but one must also know the military usage with its frequent repetition and also the structure of messages. A gift for logical combination is the first prerequisite for practical decipherers. The solution of such simple substitution ciphers forms the basis for general cryptanalysis, for this reason the simplest example of decipherment has been treated thus in detail.

But with the decipherment of the message our job is by no means completed. The decrypted message is merely a "decipherment" of an "encipherment". It is absolutely essential that we both recognize and also reconstruct the basic table according to which the messages have been enciphered in order that we may not have to decrypt anew the ever changing encipherments of the system.

To spare this labor to a great degree, it is essential that every decrypted system be reduced to its basic form. For this purpose a careful analysis of the first encipherments to be interpreted and some logical thinking will suffice.

The elements (letters, marks of punctuation, and digits) entered in the table for the count after solving the message reveal the following characteristics:

1. The thirty letters of the Russian alphabet occur only in three columns of the table.
2. One column contains only the first ten letters, the next contains ten more and the third column the last ten letters of the alphabet. In a horizontal row we find A K F , i.e., the 1st, 11th and 21st letters of the alphabet.
   In another row B L H i.e., the 2nd, 12th, and 22nd letters.
   The same thing holds for the letters in the other rows.

Consequently, if we enter in the 10 x 10 table the 30 letters of the Russian alphabet, using only the first three columns, we get the same horizontal sequences:

A K F
B L H
W M Z
G N , etc.

We can also assume that the digit sequence likewise runs down the column either as 0 1 2 3 4 5 6 7 8 9 or as 1 2 3 4 5 6 7 8 9 0. Confirmation can be had when we decipher the next messages if there is a date in the text. The fourth column (marks of punctuation) cannot be filled in except for our interpretation of "period" on the A K F level. With this the basic table has been recovered, which facilitates decrypting other messages.

One's attention will always be called to the fact that in one column of the count 1 cell is heavily scored. This could only be the period. On the same level with the period we shall find the letters A K F. The three columns of letters can also be identified readily by pattern. The sequence A to I contains only a few frequent letters and the 10 cells of this column will never be scored as evenly as those of the K-U column. Moreover in the K-U sequence stands the very frequent letter O by which this column is readily recognized.

The third column of letters consists solely of relatively rare letters so that it can sometimes be confused with the digit column but these two columns will be correctly located during the course of the work.

Thus when a letter has been identified or assumed in a row, we have determined simultaneously the other two letters, a digit and a mark of punctuation.

Since in this table only five columns have entries, there will only be five different encipherment numbers (the second digit of the 2 digit group). All ten digits will appear for the rows (first digit of the digit group). When the basic table has been recovered, the key numbers can be entered vertically and horizontally as we interpret or make assumptions and these automatically result in solution.

The method of deciphering is not essentially different when other substitution tables are used except that decipherment is somewhat more complicated in the case of tables with variants.

As many examples during the German-Russian war showed, the Russian cipher clerks did not fully utilize the advantages of the tables with variants. They almost always took the same letters which resulted in a revelation of frequencies so that the messages could be decrypted easily.

It does not make any difference how the tables are enciphered, whether with 2- 3- or 4-digit groups or with letters or symbols. The frequency count will always betray the fact that we are dealing with a pure letter text. And whenever the frequency of the individual groups is available, solution is always possible. For this reason only texts of inconsequential content should be enciphered by a substitution table without variants, a rule the Russians did not follow during the war, but used these tables for important communications. The Russians handled the encipherment of these tables in the following manner:

Radio stations which worked together in one network received each day horizontal and vertical key sequences, e.g.

horizontal: 8 1 9 7 0 2 6 4 3 5

vertical: 6 7 0 2 3 1 4 9 8 5

which they placed above and at the side of the table. These individual key

sequences were issued in advance to the station for one day, for one week or for one decade (10 days). Transmission was in writing. It often happened however that some station did not get the keys promptly and asked another station for them. Then the keys were transmitted by radio, enciphered by the same table but with the old key. With this the keys were compromised and the enemy intercept service was spared the trouble of breaking the new keys.

To save sending the key sequences to the stations every day, so-called key tables were issued. Before the war each military district received its own key tables (e.g., MVO = Moscow Military District, KyO = Kiev Military District etc.), according to this all the stations of the district enciphered their messages. The period of validity of such a key table varied.

Key Table

	0	1	(2)	3	4	5	6	7	8	9
0	3	5	8	1	9	7	0	2	6	4
L	0	8	4	5	1	9	3	7	2	6
2	7	1	9	3	0	5	2	6	4	8
3	1	0	2	7	4	6	8	5	3	9
4	5	3	6	0	2	4	1	8	9	7
5	8	4	7	6	5	0	9	3	1	2
(6)	6	7	0	2	3	1	4	9	8	5
7	2	9	1	4	6	8	7	0	5	3
8	9	6	3	8	7	2	5	4	0	1
9	4	2	5	9	8	3	6	1	7	0

Keys could be chosen at will according to this table. However, in order that the receiving station might be able to know which sequences it must use for encipherment, an indicator group was profixed to the message which stated the sequences from the table. For instance a message was enciphered by the horizontal row 6 7 0 2 3 1 4 9 8 5 and the column 8 4 9 2 6 7 0 1 3 5. The indicator group was then 6 2 (see key table).

Using this table, practically every message could be enciphered by a different key. But just as every type of system in the cryptographic service had its advantages it also had its disadvantages.

Since the encipherment sequences were selected arbitrarily from the key table, it often happened that different horizontal rows were used with one and the same column and vice versa. The enemy's intercept service then had only to decipher a few rows to reconstruct such a key table. Logically the horizontal and vertical sequences of numbers could contain only the ten different numbers and thus excluded any

sequence automatically that did not belong to the table. So when a key table had been reconstructed, all the messages that had been enciphered by this table could be decrypted at the enemy intercept station just as quickly and with as little effort as at the Russian stations themselves.

The Russian radio stations used such key tables not only with the substitution table but even for other more complicated systems (code). They simply could not carry on any smoothly functioning encryption of radiograms without such key tables but these tables, which the intercept service was able to reconstruct, facilitated decipherment and saved time.

Code (Satzbuch)

During the entire war the Russian Cryptographic Service in addition to the various substitution tables used codes exclusively. These code books differed both in structure and in the types of encipherment. The code books were put up in book form and contained from five to one hundred or more pages. Each page of the code book was divided into 50 to 100 lines. The structure of the code books varied. Here we are giving some of the main variants (see also Supplement I).

Structure of the Codes

Variant 1: The letters were introduced in alphabetic sequence on the first or last page of the code. Then followed the most common words, also in alphabetic sequence. At the end of the code came numbers, clock times, marks of punctuation, types of aircraft, types of motor fuel, troop units, compass points and to some extent names of places and commanders. These simple codes contained ten pages at most and since for the most part only letters and occasional words were taken from them, they were frequently classified as expanded Cäsars.

Variant 2: On the first page of the code was an expanded alphabet, i.e., letters, digraphs and syllables in alphabetic sequence. The rest was as in Variant 1. This type also was one of the simple codes and rarely contained more than 10 pages.

Variant 3: Page 1, row 1 began with the letter A, then followed words with that initial, then B with words beginning with B, etc. At the end it was like Variant 1.

Variant 4: The whole code was made up of digraphs, syllables, words and short sentences. There were no letters. If a letter was required in the text, it was necessary to insert a group from the code known as a "switch group" which signified "read letter". After this group only the initial letters of the code elements could be read. This avoided having the letters used in the text show any frequency because they were taken at will from words with the same initial letter. When after the letter text words were to be used once more, it was necessary to insert a switch group with the meaning "read word". Then the words from the code would be read as before. These switch groups were enciphered like all the other words in the code. This variant was strictly alphabetic but sometimes there were interruptions of the alphabetic sequence. The words under a given initial would be in strict alphabetic sequence but otherwise the vocabulary was not alphabetic, e.g., you might have first the words beginning with K, then those beginning with S and then those beginning with R, etc. Otherwise things were as already described.

Variant 5: First came the letter A with digraphs, syllables, words and sentences beginning with A in alphabetical sequence, then those with B, etc. The numbers were distributed irregularly throughout the entire book. The end was the same as in Variant 1. These code books contained 50 to 100 pages and were among the more complicated systems.

Variant 6: Each page of the code was divided into three columns. In each column stood the same letters, syllables and words in alphabetical order but not beginning with the same row, i.e., the first column began with A in row 5 and continued throughout the code book in the same manner as Variant 4. The second column began with A in

Row 2, the third with A in row 8, so that the same letters, syllables and words stood in different rows in the three several cases. These columns were designated by three different colors: red, blue, and green and had to be indicated in the message along with the encipherment.

All six variants are illustrated in Supplement I.

These codes were enciphered in different fashions. The most usual types of encipherment were not coupled with any particular type of code but might be used with any code.

Types of Encipherment and Decipherment.

1. Page encipherment.

This simplest type of code encipherment (with code book up to 10 pages at most) might be compared to the encipherment of the substitution. Each page, which was subdivided into ten quadrants with ten rows each, was enciphered with a single digit. The second number enciphered the ten quadrants and this remained the same for all pages of the code. The third number, representing the row, remained constant. Hence all elements of the code were expressed by a three digit number of which two digits were always being newly enciphered while the third always remained the same.

2. Quadrant encipherment.

Each page of the code book was divided into ten "quadrants", i.e., there were 100 quadrants for a code book with ten pages. Each quadrant was enciphered with a dinome. The rows of each quadrant (i.e., the third number) usually remained constant or, if they were also enciphered, the encipherment numbers for the ten rows of each quadrant always remained the same.

3. Encipherment tables.

Code books with more than ten pages were naturally enough enciphered with 4-place numbers. Each page and each row of the code book would be expressed then by a dinome (00 to 99). Encipherment of the 100 rows on each page remained the same for all the pages. For this, special enciphering and deciphering tables were employed. There were two tables each with 10 x 10 cells which were changed constantly.

Table A (encipherment)

	0	1	2	3	4	5	6	7	8	9
0	05	06	07	08	09	20	21	22	23	24
1	41	42	43	44	45	00	01	02	03	04
2	19	18	17	16	15	30	31	32	33	34
3	75	76	77	78	79	80	10	11	12	13
4	14	99	98	97	96	95	35	36	37	38
5	39	94	93	92	91	90	60	61	62	63
6	64	81	82	83	84	25	26	27	28	29
7	46	47	48	49	40	50	51	52	53	54
8	65	66	67	68	69	55	56	57	58	59
9	70	71	72	73	74	85	86	87	88	89

Table B (decipherment)

	0	1	2	3	4	5	6	7	8	9
0	15	16	17	18	19	00	01	02	03	04
1	36	37	38	39	40	24	23	22	21	20
2	05	06	07	08	09	65	66	67	68	69
3	25	26	27	28	29	46	47	48	49	50
4	74	10	11	12	13	14	70	71	72	73
5	75	76	77	78	79	85	86	87	88	89
6	56	57	58	59	60	80	81	82	83	84
7	90	91	92	93	94	30	31	32	33	34
8	35	61	62	63	64	95	96	97	98	99
9	55	54	53	52	51	45	44	43	42	41

To make it more convenient for the code clerk the dinomes were not entered in the tables in random fashion but according to some system. These encipherment tables were employed for the most part for the large Commander Codes. The application of these two tables was simple.

Table A was used for enciphering radiograms. Suppose, for instance, the word "aerodrom" = airfield is to be enciphered and suppose the word stood on page 02 in row 14, then from Table A the key number is taken from the interception of horizontal 0 and vertical 2. This number 07 then became the encipherment number for page 02. In the same way one proceeded with the row number 14. The resulting key number 45 came from the first horizontal and the fourth vertical sequence of Table A.

As we see, the code clerk could encipher both the page and row with key numbers from the same table. The word "aerodrom" in this case would be identical with the group 07[illegible].

Decoding of the group 0[illegible]45 was accomplished in like manner. For this Table B was used. Horizontal 0 and vertical 7 in the table yielded the number 02 and horizontal 4 and vertical 5 gave the number 14, hence 0214 = page 02, and row 14 in the code, = "aerodrom".

VARIANT 1 Supplement I

Ø1	Ø2	Ø3	Ø4	Ø5	Ø6
Ø А	Ø ВЫЛЕТ	Ø КА	Ø ОТВЕТ	Ø ПРОТИВНИК	Ø ТРО
1 Б	1 ВЫСОТА	1 КАЖД	1 ОТДЕЛ	1 ПРОШУ	1 ТЫСЯЧ
2 В	2 ГДЕ	2 КАК	2 ОТПРАВК	2 РА	2 ТЯЖЕЛ
3 Г	3 ГОДН	3 КАРТ	3 ПАРАШУТ	3 РАБОТ	3 УБИТ
4 Д	4 ГРУЗ	4 КЕМ	4 ПЕ	4 РАДИО	4 УДАР
5 Е	5 ДАЛ	5 КИЛОМЕТР	5 ПЕРЕД	5 РАДИСТ	5 УЖЕ
6 Ж	6 ДАНН	6 КЛЮЧЬ	6 ПЕРЕГОВОР	6 РАЗ	6 УМЕНЫЙ
7 З	7 ДВ	7 КО	7 ПЕРЕДАТЬ	7 РАЙОН	7 УЧЕБ
8 И	8 ДЕЛ	8 КОГДА	8 ПЕРЕЛЕТ	8 РАМЕН	8 УШ
9 К	9 ДЕНЬ	9 КОД	9 ПЕРЕМЕН	9 РЕ	
Ø Л					

VARIANT 2

Ø1	Ø2	Ø3	Ø4	Ø5	Ø6
Ø А	Ø ВИД	Ø ИДЕТ	Ø НЕМЕДЛЕННО	Ø ПОШЛИ	Ø СОСТАВ
1 АБ	1 ВНОВЬ	1 ИМЕЕТ	1 НЕТ	1 ПРАВ	1 СОСТОЯН
2 АВ	2 ВОЕНН	2 ИНЖЕНЕР	2 ОБЛАЧНО	2 ПРЕДНАЗН	2 СПЕШН
3 АМ	3 ВОЗДУК	3 ИСТРЕБИТЬ	3 ОТВЕТ	3 ПРЕКРАТИТЬ	3 СРОЧН
4 АН	4 ВСЕ	4 КАЖД	4 ОКОЛО	4 ПРЕРВАТЬ	4 ТАБЛИЦА
5 АТ	5 ВТОР	5 КАК	5 ОПЕРАТИВ	5 ПРИЕМ	5 ТАЖЕ
6 Б	6 ВЫДАТЬ	6 КАРТ	6 ОТВЕТ	6 ПРИКАЗ	6 ТАК
7 БА	7 ВЫЛЕТ	7 КЕМ	7 ОТДЕЛ	7 ПР	
8 БЕ	8 ВЫСОТА	8 КИЛО	8		
9 БИ	9 ГД				

VARIANT 3

Ø1	Ø2	Ø3	Ø4	Ø5	Ø6
Ø А	Ø ГРУЗ	Ø ИМЕТЬ	Ø МЕХАН	Ø ПОЛ	Ø РУБЕЖ
1 АВИО	1 Д	1 ИМУЩЕСТВ	1 МИНУТ	1 ПОЛЕВ	1 РЯД
2 АВТОМАШ	2 ДА	2 ИНЖЕНЕР	2 МНОГО	2 ПОЛЕТ	2 С
3 АППАРАТ	3 ДАЛ	3 ИСТРЕБИТЕЛ	3 МОЖН	3 ПОЛЖ	3 СА
4 АРМИЯ	4 ДАЛЬНЕНШ	4 К	4 МОСТ	4 ПОЛН	4 САМОЛЕТ
5 АЭРОДРОМ	5 ДАНН	5 КА	5 МОТОР	5 ПОЛОСА	5 САН
6 В	6 ДЕНЬ	6 КАЖД	6 Н	6 ПОМ	
7 ВА	7 ДИВИЗИЯ	7 КАК	7 НА		
8 БАЗА	8 ДАЛ	8 КАРТ			
9 БАЛ					

VARIANT 4

Ø1	Ø2	Ø3	Ø4	Ø5	Ø6
Ø КА	Ø БУДЕТ	Ø МЕТР	Ø ЕЩЕ	Ø ПРОЛЕТ	Ø
1 КАВАЛЕРИ	1 БЫЛ	1 МИНУТ	1 ЕЮ	1 ПРОТИВНИК	1 ЧИТ. БУКВЫ
2 КАЖД	2 БЫТЬ	2 МНЕ	2 ВАМ	2 ПРОЧН	2 ЧИТ. СЛОВА
3 КАК	3 РА	3 МНОГО	3 ВАШ	3 ПРОШУ	3
4 КАПИТАН	4 РАБОТ	4 МОСТ	4 ВЕДУТ	4 УБЕЖД	4 Ø1
5 КАРТА	5 РАДИО	5 МОТОР	5 ВЕРН	5 УБИТ	5 Ø2
6 КЕМ	6 РАДИСТ	6 АВИО	6 ВЕС	6 УДАР	6 Ø3
7 КИ	7 РАЗ	7 АВТОМАШ	7 ВЕТЕР	7 УЕХАЛ	7 Ø4
8 КИЛОМЕТР	8 РАЗДЕЛ	8 АППАР		8 УЖЕ	8
9 КЛЮЧЬ					

VARIANT 5

Ø1	Ø2	Ø3	Ø4	Ø5	Ø6
Ø А	Ø Г	Ø ЗЫ	Ø МЕР	Ø ПЕРЕГОВОР	Ø ПРИЧИСЛН
1 АБ	1 ГА	1 И	1 МЕСТ	1 ПЕРЕДАТЬ	1 ПРИШЛИТЕ
2 АВ	2 ГАЗ	2 ИБ	2 МЕСЯЦ	2 ПЕРЕДВИГ	2 ПРО
3 АВИО	3 ГДЕ	3 ИВ	3 МЕТР	3 ПЕРЕДЕЛ	3 ПРОБЕГ
4 АВТОМАШ	4 ГЛУБОК	4 ИГ	4 МЕХАН	4 ПЕРЕЕЗД	4 ПРОБН
5 АВТОПОРТ	5 ГО	5 ИД	5 МЕШАЕТ	5 ПЕРЕКИМ	5
6 АЕ	6 ГОД	6 ИДЕТ	6 МИ	6 ПЕРЕКЛЮЧ	
7 АИ	7 ГОДН	7 ИЕ	7 МИНУТ	7 ПЕР	
8 АЛ	8 Г		8 МН		
9 АМ					

VARIANT 6

Ø1			Ø2			Ø3			
Ø			Ø ГРУЗ	ДА	ГО	Ø ИЯ	КАЖД	ИС	Ø
1			1 ГУ	ДАЛ	ГОДН	1 К	КАК	ИСТРЕБИТЬ	1
2	А		2 Д	ДАЛЬН	ГОРОД	2 КА	КАРТА	ИТ	2
3	АВ		3 ДА	ДАМ	ГРУЗ	3 КАЖД	КЕМ	ИЯ	3
4	АВИО		4 ДАЛ	ДАНН	ГУ	4 КАК	КИ	К	4
5 А	АВТО		5 ДАЛЬН	ДАТЬ	Д	5 КАРТА	КМ	КА	5
6 АВ	АЕ		6 ДАМ	ДВ	ДА	6 КЕМ	КО	КАЖД	6
7 АВИО	АМ		7 ДАНН	ДЕ	ДАЛЬН	7 КИ	КОД	КАК	7
8 АВТО	АН	А	8 ДАТЬ	ДЕЛ	ДАМ	8 КМ	КОМ	КАРТА	8
9 АЕ	АП	АВ	9 ДВ						

NOTES

These different types of essentially small code books were somewhat different in their original form. When the pages of the several codes were broken up into 100 rows or into 10 x 10 quadrants or simply into ten big squares, where the separate elements were entered, the code always retained its book form with a varying number of pages. The simple types, which were divided into ten great squares on each page, were called by the Russians themselves "code table" (Kodowaya Tablitsa). These were enciphered just like all other code books, i.e., the pages were enciphered by a dinome and the quadrants by a third digit. All these six variants contained no more than 10 pages and could be enciphered with three digits. The larger codes, such as OKK-2 (Osobyj Kommandirskyj Kod = special commander code) was essentially the same code only it had 50 pages and a correspondingly larger vocabulary than these ten page codes. Through the fact that this OKK-2 had more than 10 pages, 3 digits no longer sufficed for encipherment and the texts in this code had to be enciphered by two dinomes, the first dinome for the page, the second for the row. An essential point about any complicated code was its extent and the type of encipherment to be used with it. The different types of encipherment are discussed in a separate part.

These types of table systems were in great favor among the Russians. However, essential weaknesses were inherent in them which gave the cryptanalyst a chance to lighten his labors.

For instance, if in the code on page 03 row 25 there is a frequent letter V and if conversely on page 25, row 3 there is another frequent letter or digraph, say NA, then these two elements of the code would always look the same however they might be enciphered: 0830 - 3008, or 7249 - 4972, etc. If a code had several such parallel passages, the cryptanalyst could recognize these so-called mirror groups immediately in the enciphered message. There are such parallel passages in every code. The cipher section in Moscow, where all cryptographic systems and keys were compiled, paid no attention to these little weaknesses, otherwise it would have avoided them.

Since the encipherment from one table would not have sufficed for disguising messages very long, ten to twelve such double tables were issued simultaneously which could then be used in alternation. In order that the cipher clerk might know when deciphering a message which of these ten to twelve tables he was to use, each table was designated by a 4-digit group, the so-called indicator group. Ahead of each enciphered text must always stand the indicator showing the encipherment table used.

Tape Encipherment (Bandrollen-Verschlüsselung)

Basically this type of encipherment is the same as the encipherment table. The pages and rows of the code were enciphered by dinomes, only the use of the key was different and the roll did not have to be changed frequently. The entire code was divided into two halves of 50 pages each - the left and right half of the code. The firm pasteboard covers of the code book were considerably broader at the side than the pages of the book itself. On these broad margins of the cover were attached two so-called "pockets" which were just as tall as the pages of the code.

For each encipherment two rolls were required - a left and a right. These rolls contained ten different vertical sequences of dinomes.

The code books for which such encipherment was intended had a special structure. Each page of the code was, like the code itself, divided into a left and right half page. Thus each page had two sequences of rows numbered 00-24 and 25-49 or 50-74 and 75-99.

(For details see Supplement II).

Supplement II

50 - Page Code Book

37	Ø2	Ø1	КИДАТЬ	26	КУДА СООБЩ.	51	ЛИХ	76	МЕ	56	99
38	Ø3	Ø2	КИЛО	27	КУСТ	52	ЛИЧН	77	МЕДИЦИН	57	75
39	Ø4	Ø3	КИЛОГРАМ	28	КУЧЕВАЯ	53	ЛИШН	78	МЕДЛЕНН	58	76
25	1Ø	Ø4	КИЛОМЕТР	29	Л	54	ЛО	79	МЕЖДУ	59	77
26	11	Ø5	КИСЛОТА	3Ø	ЛА	55	ЛОДКА	8Ø	МЕЛ	7Ø	78
27Ø4	12	Ø6	КЛАСТЬ	31	ЛЕ	56	ЛОЖН	81	МЕЛК	71 12	79
28	13	Ø7	КЛАССОВ. БОРЬБА	32	ЛЕВ	57	ЛОЖН. ТРЕБОГА	82	МЕН	72	9Ø
29	14	Ø8	КЛИМАТ	33	ЛЕГКИЙ	58	ЛОМ	83	МЕНЬШ	73	91
4Ø	21	Ø9	КЛЮЧЬ	34	ЛЕД	59	ЛОПАТ	84	МЕНЯ	74	92
41	22	1Ø	КЛЮЧЕВ. ТАБЛИЦА	35	ЛЕЖАТ	6Ø	ЛОШАТЬ	85	МЕРА	65	93
42	23	11	КРАЙ	36	ЛЕЖИТ	61	ЛУ	86	МЕРОПРИЯТИЕ	66	94
43	24	12	КРАН	37	ЛЕЙ	62	ЛУГ	87	МЕРТВ	67	8Ø
44	15	13	КРАСКА	38	ЛЕКАРЬ	63	ЛУН	88	МЕСТ	68	81
3Ø	16	14	КРАСН	39	ЛЕНИН	64	ЛУЧЬ	89	МЕСЯЦ	69	82
31	17	15	КРИВОЙ	4Ø	ЛЕС	65	ЛУЧШЕ	9Ø	МЕТЕО	5Ø	83
32Ø4	18	16	КРОМЕ	41	ЛЕТ	66	ЛЫ	91	МЕТЕО СВОДКА	51	84
33Ø4	19	17	КРУГ	42	ЛЕТАТЬ	67	ЛЬ	92	МЕТР	52 12	89
34	2Ø	18	КРУПА	43	ЛЕТЕТЬ	68	ЛЬН	93	МЕХ	53	88
45	Ø5	19	КРУТ	44	ЛЕТН	69	ЛЯ	94	МЕХ. РОТА	54	87
46	Ø6	2Ø	КРЫШ	45	ЛЕТЧИК	7Ø	М	95	МЕХАН	6Ø	86
47	Ø7	21	КТО	46	ЛЕТЯТ	71	МА	96	МЕШАТЬ	61	85
48	Ø8	22	КУДА	47	ЛИ	72	МАЛ	97	МИ	62	95
49	Ø9	23	КУДА ВЫСЛАТЬ	48	ЛИНИ	73	МАРТ	98	МИЛ	63	96
35	ØØ	24	КУДА НАПРАВИТЬ	49	ЛИСТ	74	МАСЛО	99	МИМО	64	97
36	Ø1	25	КУДА ПРИСЛАТЬ	5Ø	ЛИТЕР	75	МАСС	ØØ	МИР	55	98

This code book was divided into two halves. The left and the right half each included 25 pages. Each page was divided into four parts with 25 rows each 01 to 25, 26 to 50, 51 to 75 and 76 to 00. The left and right side of the code were enciphered by a different key roll. For this purpose the left or right dinome of the table could be selected. For the rows one took for 01 to 25 the first digit sequence of the left key table, for 26 to 50 the second, for 51 to 75 the first row and for 76 to 00 the second row of the right key table. The keys were designated in the message by two indicator groups, e.g., in this case the first number at the top of the first digit sequence at the left "37" and the middle red number "04" = indicator group 3704, then the first number at the top of the first right hand sequence "56" and the middle red number "12" iindicator 5612. Ahead of the cipher text stood therefore the two indicator groups: 3704 5612. The code clerk knew that the first indicator group was for the encipherment of the left side and the second for the encipherment of the right side of the code book. This type of encipherment and the structure of the code could, however, reveal the following weaknesses:

1. If the key rows were unknown and some element or other from the code could be interpreted, e.g. the letter "M" = 3360, then it could be stated with certainty that all 4-place groups with the same encipherment which began with 00 to 49 could only be the first half of the code, i.e. the alphabet from A to N, and the other groups which began with 50 to 99 could only be the other half of the code, i.e., from O to the end of the alphabet. This division helped materially in solving the new key rolls.

2. Since each page was likewise divided into four parts, the subdivision of the left and right half could also be carried out, which resulted in narrowing down the choice of the code elements on each page.

3. Since the key sequences in the two rows were so drawn up that they revealed a certain systematic character, e.g., 05 06 07 08 09 00 01, etc., these key numbers could be reconstructed if a number here or there was identified, e.g., if the key number 60 was identified for the row 70 (M) of the code, a key number 61 for 71, 62 for 72, 63 for 73, 64 for 74 might be assumed. At the same time the 5-key numbers were fixed for the five pages of the code.

4. Since each page could be expressed by the left hand or the right hand double key number, e.g., page 17 by 19 and 33, the two key sequences could be reconstructed in part on the basis of these two numbers:

16 30 for page 14 line 14 and 39
17 31 " " 15 " 15 and 40
18 32 " " 16 " 16 and 41
19 33 " " 17 " 17 and 42
20 34 " " 18 " 18 and 43.

The correctness of the assumption could always be confirmed by solving other messages. This regular numerical sequence of at least 5 successive dinoues was selected in order to somewhat lighten the labor of the code clerk when enciphering or deciphering the messages. If the numbers had been thoroughly scrambled, then the search for the key numbers would have taken a great deal of time. For this reason this facilitation was introduced, but it facilitated simultaneously the work of the cryptanalyst.

In the later years of the war these types no longer appeared.

Encipherment Roll

07	04	33	10	47	24	27	18	43	21	48	
08	05	34	11	46	00	28	17	44	22	49	
08	11	35	12	45	01	29	16	45	23	25	
10	12	25	13	25	02	41	15	31	24	26	
11	13	26	14	26	03	42	00	32	15	27	
12	14	27	00	27	04	43	01	33	16	28	
13	15	28	01	28	10	44	02	34	17	29	
14	20	29	02	29	11	45	03	34	18	40	
15	21	46	03	41	12	36	04	29	19	41	
16	22	47	04	42	13	37	24	28	00	42	
17	23	48	20	43	14	38	23	27	01	43	
18	24	49	21	44	05	39	22	26	02	44	
19	06	36	22	20	06	40	21	25	03	30	Left key roll
20	07	37	23	31	07	46	20	36	04	31	
21	08	38	24	32	08	47	05	37	05	32	
22	09	39	15	33	09	48	06	38	10	33	
23	10	45	16	34	19	49	07	39	11	34	
24	16	44	17	35	18	30	08	40	12	39	
00	17	43	18	40	17	31	19	30	13	38	
01	18	42	19	39	16	32	14	46	14	37	
02	19	41	05	38	15	33	13	47	06	36	
03	20	40	06	37	20	34	12	48	07	35	
04	01	30	07	36	21	35	11	49	08	45	
05	02	31	08	39	22	25	10	41	09	46	
06	03	32	09	48	23	26	19	42	20	47	

After these last numbers the same numbers follow in the same sequence as above. When an encipherment is chosen, e.g., 1604, then the roll was so placed that the upper horizontal sequence began with the indicator number 16 and the left hand and right hand column of "04" remained visible as the outermost encipherment sequences. The rest of the row, which was to the right of "04", was actually concealed in the pocket of the code book. The right key roll with the dinomes 50 - 99 was set up in the same manner. (See also Supplement II).

This type of encipherment gave the code clerk a possibility of selecting a large number of variants from the different key sequences and thus extending the use of the two rolls over a relatively long period. These encipherment rolls had one other advantage, that the pages of the code book could be expressed by two dinomes. However this was very rarely done, which again reflects the carelessness of the Russian radio personnel. The weaknesses of this type of encipherment are described in detail in Supplement II.

Interval Encipherment
(Intervallen-Verschlüsselung)

Interval [or range] encipherment was based on the same principle as the tape encipherment. The rolls were the same and the use was the same. It was the commonest type of encipherment used by the Russian Air Force, in particular during the later years of the war.

This type of encipherment was the simplest and nevertheless the cleverest type produced by the Russian cryptographic service. If messages had been enciphered exactly according to regulations, it would have been almost impossible to decipher them. But that did not happen and the encipherment lost all value.

The key sequences were constructed on the same principle as the tape encipherment, as has been mentioned already. Of course the key sequences were made up in an entirely different fashion. They did not contain one diresne to be used for the encipherment of the pages or rows of thecode but were constructed as follows:

23-27	91-94	02-05	16-19	
28-31	95-99	06-09	20-24	
32-35	01-04	26-29	73-75	
36-40	05-09	30-34	76-79	
41-44	00 20-24	00 46-49	00 80-83	
45-49	25-27	50-54	84-86	4 to 6 additional sequences
11-15	28-31	55-59	87-90	of the same type
16-20	32-35	15-18	06-09	
75-79	71-73	19-21	10-14	
80-84	74-77	22-25	21-24	
55-58	78-80	83-85	25-28	
59-61	15-19	86-89	29-32	
62-65	87-89	41-45	33-35	etc.

With these interval key numbers, e.g., 23-27 the clerk could encipher the element of the code book not merely with a number 23 but optionally with the numbers 24,25,26 and 27. By this method all repetitions could be avoided in the text and there would hardly have been any frequencies appearing. Instead there would have been a fairly even score for all letters, syllables and words and it would have been very difficult to solve the messages, to say nothing of the codes themselves.

The Russian clerks however failed to take full advantage of this possibility. When enciphering, they found it more convenient to take only the numbers that were printed on the key roll, e.g., 23 and 27, 28 and 31, etc. The remaining numbers lying between those printed on the roll were used but rarely so that the count made of such messages revealed clearly the frequency of the first and last groups, between which other numbers appeared only sporadically.

The cryptanalyst did not find it difficult to get the limits of these intervals and to reduce the groups, say 23 to 27, to a common denominator. Then the key sequences could be treated in the normal way and decryption resulted just as in the case of the tape encipherment.

Additive system

The code books enciphered by the additive system contained more than 100 pages and were used only by the higher staffs. The message text was enciphered by three types of keys:

1. Normal blocks [pad sheets reused].
2. Individual blocks [pad sheets used once only], and
3. Central blocks [circular?].

The most common were the normal and individual blocks. The central blocks were hardly used and need not be considered.

The normal block contained 10 different key tables, each of which could be employed several times. Each key table contained 5-digit groups in rows of 8 to 10 groups and with as many as ten rows.

57210 84409 68421 00857 19972 25489 11795 00076
90162 39014 88391 53820 35428 87635 38922 45362
97537 36728 93873 10009 90080 31133 40139 89653
35241 11993 36287 90134 23498 97685 07923 64529
29384 60011 39801 25437 09098 25911 38921 59201
10009 93721 76548 46387 93873 44559 34672 83011
34629 05380 25631 66473 34233 57748 00187 38708
64873 99938 01394 48746 66663 01945 88466 39826
15557 38762 36457 58236 49999 36537 11133 39873
75756 35672 39873 00013 83764 94848 53465 39000

Each table contained a 5-place number. Each block, which contained 10 such tables, was indicated by five digits. These block and key table numbers had to be introduced into the message as indicator groups in order that the decoder might know which table he was to use to decipher the message.

Encipherment of the messages was as follows: The code numbers (pages and rows of the code) which yielded the text, were taken out in sequence so that the 5-digit groups stood 8 in a row. Then the key table is so applied that a key group stood beneath each code group. This key group was then added to the code group without carrying the tens.

Example:

Message Group	11012 01471 61993 70516 73088 37519 20007 20694
Code Group	83376 90094 36527 49487 36453 99883 90014 93001
Key Group	38746 11487 35476 31139 47635 48736 30093 37693

The 5-digit groups at the top were the enciphered code groups. If a message had more groups than were contained in the key table, the groups of the key table were used again, starting at the beginning, which resulted in an uninterrupted sequence of group numbers. This give rise to the name "Zahlen-Wurm" (number worm=additive sequence).

In order that a key table might be used several times, a different starting point was chosen for each message. This starting point also had to be sent along with the indicator groups. All messages enciphered by one key table belonged to a "series", i.e. all messages of one "series" could be grouped together and worked on together in the cryptanalytic section.

Decipherment of such messages proceeded in a similar fashion.

Example:

Cipher Group	11012 01471 61993 70516 73088 37519 20007 20694
Key Group	38746 11487 35476 31139 47635 48736 30093 37693
Code Group	83376 99094 36527 49487 36453 99883 90014 93001

In deciphering, the key table was also applied to the enciphered groups but instead of being added was subtracted.

The weaknesses of such key tables (normal blocks) resulted from the fact that the cryptanalysts (i.e., the enemy intercept service) could combine in one "series" the messages enciphered by any one key table and if there were

more than four messages in a "series" he could also decipher them. These were the disadvantages of the normal block. Consequently these tables were only employed because one could use a block (10 key tables) for a relatively long time and no current supply of new blocks was necessary.

The individual block also contained 8 to 10 key tables with 5-digit groups. The groups of the key table were added or subtracted just as in the case of normal blocks. The only difference is in the use of the two types.

It was forbidden as a matter of principle to encipher more than one message with one and the same key table from an individual block. If the message were longer than the table, the next table had to be taken to piece out. Since each key table was always used beginning with the first group, the starting point, which could be chosen variously (in the case of normal blocks) dropped out. The indicator group only showed the number of the block and of the table. Only in rare cases during the war was it possible to find two or three messages enciphered by one and the same key table. This probably happened for the simple reason that the radio station had not received any new individual block and was forced to encipher its messages with key tables that had already been used.

For this reason decipherment of messages enciphered by the individual key tables was impossible. The only question was whether the stations which were supposed to encipher their messages with these individual blocks would get an adequate current supply. That might be possible in the case of the higher staffs which were far removed from the battle line. The question of supply was more difficult in the case of other units which were constantly on the move and were exposed to the risk of letting cryptographic material fall into the hands of the enemy. Furthermore, in the case of mobile units replacement of the many blocks was less easy so that smaller units often worked with more simple codes and keys. Nevertheless, during the war many big codes with countless blocks (individual and normal) fell into German hands.

The great advantages of the additive keys was that in enciphering the code group by adding the key group, any repetition was avoided. Thus if one and the same group of the code occurred repeatedly, it was changed each time by the key group added to it. This resulted in a completely false statistical picture with which nothing could be undertaken. Only in the case of normal blocks, when one table was used for several messages and these messages were then lined up correctly, was it possible to decrypt them using an especially prepared difference catalogue. Only during the first two years of the war did the Russians use normal blocks predominantly, later they virtually disappeared and only the individual blocks were used.

Solution and Structure of the Basic Code

To illustrate the solution of a code, we must start with an example. For this purpose we shall select a simple Air Force code, one of those which the Russians used during the war.

The structure of the code was essentially like the others. (See Supplement III).

In order not to complicate the decipherment process unnecessarily, we have chosen a simple type of encipherment.

Supplement III shows the code in its basic form. To make it easier to grasp, the code has not been reproduced in its original form but on a single sheet. Each column corresponds to a page of the code book which is subdivided into ten squares (quadrants) and each square into ten rows. The numbers entered at the top and at the side are the assumed key numbers with which the text has been enciphered.

The text selected here has been freely invented but is similar to originals. The text has been enciphered by the code (Supplement III) and has been entered above the cipher groups for purposes of comparison. The translation of the reconstructed message reads:

the first indicates the page of the code the second the horizontal square,

To the Chief of Staff of the 8th Air Army.

Please inform me as speedily as possible where we are to move our radio station because the danger of falling into the hands of the enemy is becoming ever greater. Fuel for maintaining the work of the radio station is on the wane. The receivers will shortly be unable to function.

Signal Chief of the 55th RAB Major LIVASHEV.

Cipher groups and text:

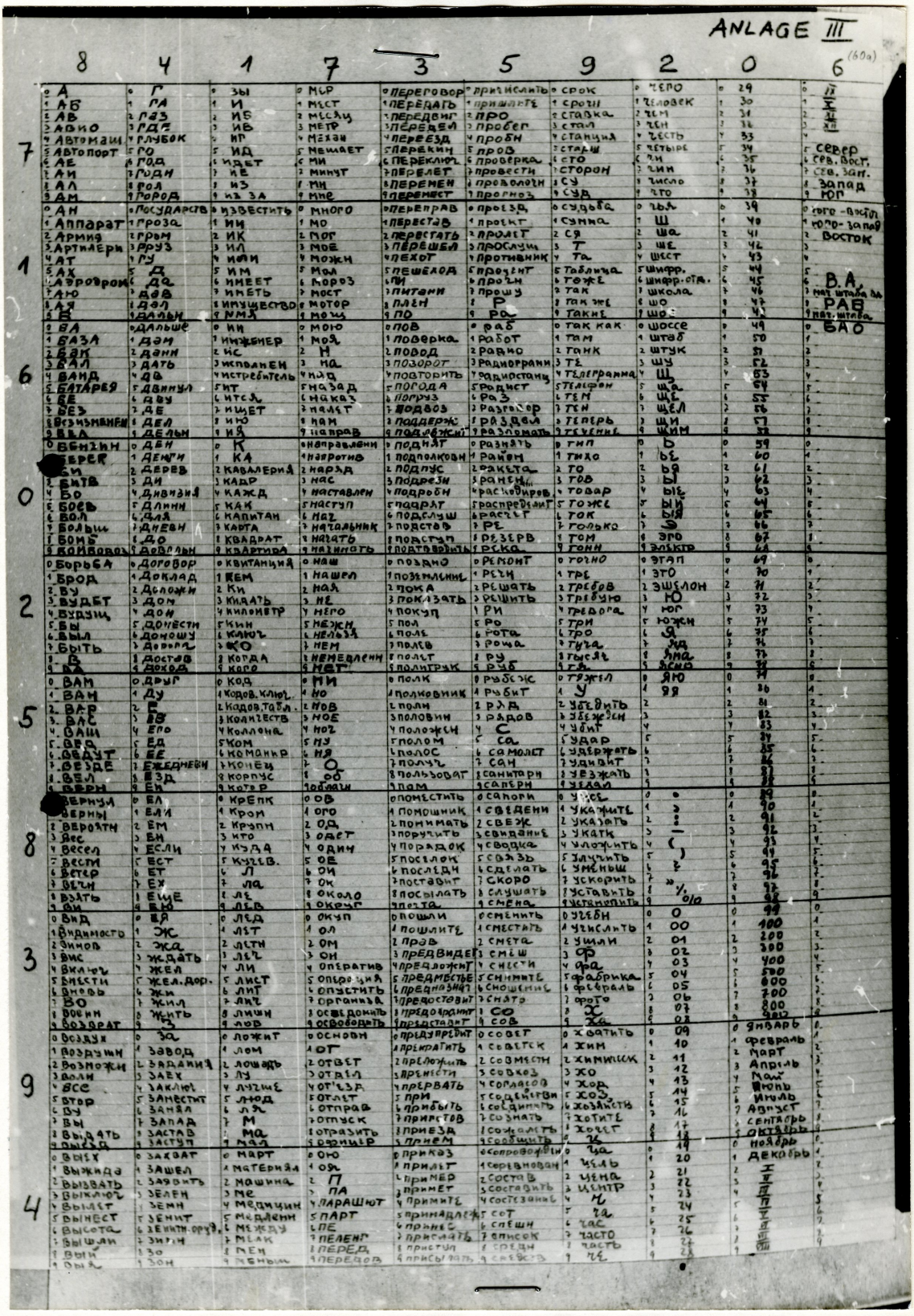
НАЧ	ШТАБ	У	8	ВА	(·)	СРОЧН	О	СООБ-ШИТЕ	КУДА	ПЕ	РЕ	БАЗ
706	261	951	239	616	280	971	757	599	184	746	507	861
И	РО	ВА	Т	Ь	НАШ	У	РАЦИ	Ю	ТАК	КАК	О	ПА
171	525	829	913	200	720	951	564	223	917	105	757	743
С	НО	С	Т	Ь	ПО	ПА	С	Т	Ь	В	РУ	КИ
554	751	554	913	200	319	743	554	913	200	828	528	122
ПРОТИВНИК	А	С	ТА	НО	В	ИТ	СЯ	ВСЕ	БОЛ	ЕЕ	ВО	З
514	870	554	914	771	828	165	912	894	906	456	837	439
МО	Ж	Н	ЕЕ	(·)	БЕНЗИН	НА	ОБ	С	ЛУ	ЖИ	ВА	Н
711	431	762	456	280	800	763	758	554	193	436	829	762
ИЕ	НАШ	ЕЙ	РАЦИИ	КО	Н	ЧА	ЕТ	СЯ	(·)	ПРИ	ЕМ	НИ
177	720	459	564	127	762	945	486	912	280	395	482	750
КИ	СКОРО	НЕ	С	МО	Г	У	Т	ДА	Л	Ь	ШЕ	РАБ
122	587	723	554	711	470	951	913	416	186	200	213	560
ОТ	АТ	Ь	(·)	НАЧ	СВЯЗИ	БЗ	РАБ	МА	Й	О	Р	ЛИ
791	814	200	280	706	585	064	618	198	171	857	518	134
ВА	Ш	Е	В	(·)								
829	211	452	828	280								

This message contains 109 groups and would naturally never be sufficient for a decipherment if the code were not already known.

the first indicates the page of the code the second the horizontal square,

SECRET

Supplement III



SECRET

Tabulated Count

	0	1	2	3	4	5	6	7	8	9
0		5КАК	0 ш ь			7 РЕ		6, НАУ	0 БСПЛИН 6 БОЛ	
1			1 Ш 3ШЕ	3ПО	6 ДА	4 ПРОГИБ НИК 8 Р	6 В.А. 8РАБ	1, МО	4 АТ	2, СЯ 3 ш Т 4 ТАУТАК
2		21 КИ 7КО	3Ю			5 РО 8 РУ		0, НАШ 3 НЕ	8 ,, В 9 ,, ВА	
3		4 ЛИ	98		1 Ж 6 ЖИ 3 З				7 ВО	
4								6 ПЕ 3, ПА		5 ЧА
5					61 ЕЕ 2 Е 3 ЕЙ	4 ЖИС		0 ИН 1 НО 7 ,, О 8 ОБ		1 ,, У
6	453	5 ИТ	1 ШТАБ			0 РАБ 4, РАЦИЯ		2 ,, И 3 НА	1 БАЗ	
7		11 И 7ИЕ			0 Г			1 НО	0А	1 СРО-ЧНО
8		6 Л 4КУДА	0 ш (·)		6 ЕТ 2 ЕМ	5 СВЯЗЬ 7 СКОРО				
9		3 ЛУ 8 МА		5 ПРИ		СООБ-ЩИТЕ 9		1 ОТ	4 ВСЕ	

The groups entered in this tabulation from the cipher message usually occur only once. The frequency of the single groups is hardly noteworthy. However this is not a case of genuine decipherment but we are merely to illustrate

1.. How a text can be enciphered,

2. How, by using the count, the code, which in its basic form is alphabetic, is torn asunder by the encipherment, and

3. How by using solved messages and the tabulated count we can recover the basic code when it is not known.

If a code is not known, we require for solution at least 20 to 30 long, carefully intercepted messages. (This holds true only for codes and encipherments such as those under consideration.)

Since the text can be put together out of words, syllables and letters, words which are repeated can be composed differently from digraphs and syllables. In this way the frequencies of the letters, syllables, letters and digraphs can be disguised and for solution more traffic is required in order to discover the frequency of the single elements.

If we look at the tabulated count, where all the code elements have already been entered in red, we can note the following:

The third digit in the group, which is entered in the various squares, remained constant, i.e., it was not enciphered. The proof is: in square -91- the digit 2 is the final element under "S" = the syllable "sya". The digit 3 is "T", 4 is "TA", 7 is "tak". The alphabetic sequence has remained here along with the sequence of the row numbers. The same thing is true of square -75-. The digit 0 is "ni", 1 is "no", 7 is "O", 8 is "OB",etc.

If the third digit had also been enciphered, then the alphabetic sequence of the letters, syllables, etc., could not have been preserved within the square.

Hence if the third digit were not enciphered, then all adjacent frequencies like 8 = "V" and 9 = "VA" in square -2- would always reappear with different encipherments. Since letters and digraphs like V and VA, D and DA, K and KA, M and MA, N and NA etc. are often employed when using code books, the adjacent numbers which express these letters and digraphs will also attract attention by their frequency in the tabulated count, Hence if "O" (the most frequent letter in the Russian alphabet) has been interpreted in this case as square -75- digit 7, and in the same square there is also the digit 8, we can say with almost 100 percent certainty that this represents the syllabde "OB". Moreover the digits ahead of 7, the digits 0 and 1 cannot come into the range of the O letters but must signify something beginning with N and since it is ahead of the letter "O" it must be something beginning with "NI.." or "NO..".

These assumptions can help a great deal in solving the message because in the beginning every assumption is important. Let us assume that the group 554 which appears several times in the message has been interpreted as "S". In the third digit sequence of the message we find between the two 554 groups the group 751. Group 751 is a group standing ahead of "O" (757), hence might be something beginning with N... . Presumably it can be a digraph and not a word starting with N and since it comes a short ways before the group for the letter "O" we may assume that we have either NI, NO or NU. This assumption we enter between the two "S" and look at the groups ahead of "S". The second group ahead of "S" is 757 = "O", then comes 743 which appears twice in the count and stands in the same column 7 with "O". We assume that group 743 cannot be a syllable starting with O because two "O" in

succession and then "S" is a very rare combination and consequently our group might be either something starting "N.." (ahead of "O" or something beginning with "P.." following the letter "O").

Since in square -75- the digit 1 ahead of "O" has already been interpreted as "NO" or "NU", the number 743 might be either "NA" or "NE", or if it starts with P it might be "PA" or "PE". If we now insert between "O" and "S" the syllable "NA" or "NE" or "PA" or "PE" and pronounce all four syllables in connection with "O" and "S", then the syllable "PA" seems most plausible. We read: O PA S .. S... If we now assume the syllable between the two "S" to be "NI" or "NO", then we get the word O PA S NO S (T) signifying "danger". With this word we have also found the letter "T" and the "soft sign" after "T".

After the first break in has been made, the next interpretations are easier, e.g., in the fourth row of the message the third group is again "S" followed by 914. Group 913 was "T", hence 914 might be "TA". We have already equated 771 and "NO": S TA NO .., the following group is 828. This same group occurs once more at the end of the message and may well be the final letter of a name (signature). Many Russian names end in "V". In square 82 of the count we have two digits 8 and 9 both of which occur three times and consequently might well be "V" and "VA". This assumption fits in well with the groups already interpreted: S TA NO V .. ... The next group following "V" is 912. Group 913 has been interpreted as "T". 912 must be the last syllable beginning with "S" and this is generally "SYA". This assumption also appears correct for the partially recovered word "S TA NO V .. SYA" can only be STANOVITSYA = "begins". Consequently group 165 is "IT" and 912 is "SJA".

In the third row of the message we find once more the group 554 and 913 200 which we have interpreted as S T and the "soft sign". The group ahead, 743, is known as "PA", hence .. PA S T ' with the already recovered word OPASNOST' (danger) ahead of it can only suggest 'POPAST' and the phrase is "run into danger".

And so we continue. If the first break has been made and if the text is made up in part of letters and syllables, further solution becomes more and more easy.

Of course the syllables and the digraphs can disturb the frequencies which would be revealed by letter text, but once the first digraphs or syllables have been interpreted, they facilitate further solution. In this way groups that occur only rarely in the count may be solved.

Further study of the tabulated count shows the possibilities:

1. Of arranging alphabetically the code which has been torn asunder by the encipherment, i.e., of restoring it to its basic form, and
2. Of recognizing the system of encipherment.

After studying the individual columns (pages) of the count, we recognize that in column 8 stand the letters A,B and V, consequently this will be the first page of the code. Then comes column 4 with D,E as page 2, then column 1 with I, K, L, M as page 3, then column 7 with M, N, O, P as page 4, then column 3 with P as page 5, then column 5 with P, R, S = page 6, then column 9, S, T, U as page 7, and column 2 with Sh and "period" as page 8, Finally we have two columns left (6 and 0) which cannot be placed for the moment because we cannot know which one of them is supposed to be the final page.

After the vertical sequence of the pages has been obtained (1 = 8, 2 = 4, 3 = 1, 4 = 7, 5 = 3, 6 = 5, 7 = 9, 8 = 2) we must proceed in precisely the same manner with the horizontal rows.

We start with the assumption that "A" stands on the first page in the first row, then the 7th horizontal row = 1; the 1st = 2; 6th = 3; the 0th = 4; the 2nd = 5; the 3rd = 6; the 9th = 7; the 5th = 8; the 8th = 9 and 4th = 10.

After we have reduced this code in its alphabetic sequence to the basic form, other new encipherments can be compared horizontally and vertically with the several columns of the code just as in the case of the substitution tables. In case the encipherment number should not change, the second digit of the group signifying the square "V" and "VA" would at the same time indicate the squares "ME", "RO", "RU", "KI" and "KO". The same thing holds with respect to other squares.

This is true only of the simplest type of encipherment if the encipherment numbers function as follows:

the first indicates the page of the code the second the horizontal square, and the third remains constant. This simple type of encipherment was used before the war and only rarely during the war. However the fundamental idea

for the solution of the more complicated encipherments is not essentially different. Only the solution of a new code becomes more difficult, the decipherment of additional messages, once the code has been solved and reduced to its basic form, remains the same.

All the difficulties in solving new codes arose simply because of

1. The extent of the code and the manner in which it was constructed, the way the messages were compiled and encoded, and
2. The types of encipherment employed.

If a code was very extensive and permitted the clerk to encode his texts using words, a few sentences and only occasionally syllables and digraphs and very rarely letters, then it took a lot of traffic and tedious effort to solve the code.

And even when such a code had finally been solved and reduced to its basic form, it was not always so easy to decipher messages in that code because with so rich a vocabulary the text could be enciphered differently and no frequency peaks appeared.

In the early stages newly solved codes had only a few recovered elements and messages could be read only in part. For this reason it was very important to work these codes out on the basis of the messages collected and partly solved. This called for experienced people with a good knowledge of the language, who by working the messages over again and again pieced together their little mosaic and were able to complete the texts of the messages and consequently the entries in the code.

For perfect solution of the radiograms it was not necessary to solve the code 100%. Usually when 50 to 60 percent of the groups had been recovered the cipher texts could be read satisfactorily. Experience showed that for the most part the same groups from the code were used.

The reference work compiled from the (solved) messages - several thousand were used for the purpose - contained not more than 20 pages with 100 lines to a page, i.e., a total of only 2000 different code elements (syllables, words and occasional sentences) although the larger code books (Commander Codes) had as a rule 50 to 100 pages (5000 to 10000 elements).

This reference work helped the cryptanalyst find new groups in breaking and working out the code. When a few groups had already been interpreted and unknown groups of the messages fell in empty cells of the code, the cryptanalyst could call to his aid the groups standing before and after the empty cell and for the interpretation of the unknown group look up in the reference work the entries between corresponding positions and words which fitted into the text. Since the cipher text of Russian messages was usually composed of the same words and the code books contained now more now fewer elements, it was possible to make good use of the reference work with its alphabetically arranged elements as the size and structure of the code to be solved became evident. This reference work aided the cryptanalysts greatly during the war.

It would be a mistake to take an extensive captured code book (an original code) for the purpose. To begin with, there were many groups in such a code which were rarely or never used and in the second place a number of groups, which had to be taken into account, disappeared or appeared in the new Russian codes. Use of the big code with more than 100 pages and 10,000 groups would not have enabled the cryptanalyst to pick out with fair certainty the correct meanings in the case of codes of 10 to 20 pages because he would have had too wide a choice.

Consequently the reference work, which was compiled exclusively from words occurring in solved messages and in completely solved codes, was further supplemented so that it did increase in size but did not become too big to be useful. The reference work was not constructed like a dictionary but like a fairly large code with 100 groups in alphabetic sequence on each page. Moreover on the final pages were entered all airplane types, tanks, types of fuel, etc., etc. On the final page stood numbers, clock times, points of the compass, and sometimes special, often used meteorological expressions which were always appearing in the same order in special weather messages.

Coordinates (Planquadrate)

Since very many place names occurred in the messages and since these must never be sent in clear, they were enciphered in various ways:

1. Encipherment of the place names like the rest of the text was by the use of letters or syllables or digraphs. But since a number of places might be named in one message and they could only be sent in letters and syllables, this resulted in high frequencies of the letters and syllables which greatly facilitated the work of the cryptanalyst.

2. The several troop units had listed on one page in their codes place names for their area. In this way a place could be designated by a single cipher group. However this was only practicable in peace time when the units had their fixed location and were not moving about all the while as in war time. For this reason this type of encipherment for place names dropped out almost entirely during the war.

3. The Russian army maps were divided into squares (Planquadrate) and each square into 10 x 10 smaller squares. The indication of a place was by a vertical and horizontal number which defined the square on the appropriate map and by a vertical and horizontal number which defined the square containing the place. For very precise location the square containing the place was once more subdivided into 10 x 10 squares. Then the place was expressed by a 6-digit number. These three vertical and horizontal sequences were regularly enciphered.

The 6-digit groups in the messages stood out clearly and the cryptanalyst could unhesitatingly accept them as place names. After the messages had been deciphered except for the 6-digit groups, they were worked on by special experts who were only concerned with solving the coordinates.

In new codes, when one did not yet know which units were using them, the coordinates appearing in the messages could sometimes be solved sooner than the codes and messages themselves. After the place names had been interpreted it was easier to solve the code, because the place names disclosed further details (thanks to the card file of place names, troop units and personal names kept by the Cryptanlytic Section) which were helpful in solving the code.

Decipherment of the coordinates was an extra job that had to be done but it helped with the decipherment of the code. Moreover solution of the coordinates, in cases where the new code could not be broken for some time, might serve to fix the networks and thus make it possible to direct interception of that traffic which was needed for the solution of the code. Thus the coordinates had their advantages and their disadvantages.

Errors and carelessness in the Russian cryptographic service.

Experienced gained before and during the war with the Russian cryptographic service showed:

1. Russian cryptographic personnel at the radio stations was not first class because it did not carry on its work in a conscientious fashion.

The cipher section in Moscow compiled the necessary means of encipherment and issued precise instructions as to how these codes and ciphers were to be handled. These instructions were never followed fully by the cryptographic personnel of the several radio stations. The individual code clerks made their work easy for themselves in complete ignorance of the extent to which the enemy intercept service was at work and of how easily their negligence ruined the security and serviceability of the codes and ciphers.

It is hard to say whether this was merely carelessness and fickleness. If the Russian code clerk had been occupied with practical decryption of their own messages (or those of others), they surely would not have kept repeating the same careless mistakes as they continued to do down to the end of the war. Perhaps they were not adequately trained and in their primitive manner of thinking believed that the text when sent in digits which were superenciphered in a constantly changing fashion, could not be solved quickly or perhaps not at all. It is also possible that such thoughts only occur to one who has been engaged in cryptanalysis for many years and has learned such things by experience. Nevertheless, the carelessness of the Russian

code clerk was so obvious that it could only lead to the conclusion that the Russian code clerks had been trained, but that their knowledge of cryptographic matters was still very primitive.

Of course this does not apply to the code clerks of the higher echelons who worked with the big Commander Code (additive system). They were specially chosen and specially trained men who made no grammatical errors in their cipher texts, such as occurred very frequently with the code clerks of the lower units.

Which were the mistakes which occurred most frequently? Those mistakes which were made constantly were generally in the encipherment of the text that had been turned over to them by their superior for transmission. In spite of the fact that there were many words and syllables in the code which could be used for the purpose they frequently merely spelled out the word. This made the messages longer, gave higher frequency counts for the groups and thus turned a code into an expanded substitution table, which was a fairly simple thing to solve.

This happened chiefly with those codes which had the whole alphabet on the first or last page. It was easier and simpler for the code clerk to use the groups on that page than to hunt around through the code book.

Moreover the numbers which were contained in the code were not always used. Frequently the date or clock time stood out clearly in plain text in an enciphered message. This seemingly insignificant detail really betrayed to the cryptanalyst quite a lot and in most cases he was able to interpret several groups before and after such data sent in the clear.

For instance, if the clock time was in clear in the message, the group ahead of the clock time might be interpreted as "V" (at) and the group following as "chas" (hour). Since the letter "V" in Russian not only appears in words but is often used as a preposition, this initial recovery helps in the further solution of the code. Or suppose there were two clock times, e.g., 11.30 ... 12.00. If the same group stood after each of these

it signified "chas" (hour), then the group ahead of the first clock time was "S" (from) and the group between the two was "DO" (to), i.e. "from 11.30 to 12.00 hours." Similar interpretations could be made with absolute certainty in connection with a date sent in clear. Failure to encipher clock time and date was due to indolence and the clerk never thought that this could lead to solution of the message and possibly of the code itself.

But even in the encipherment of the messages the Russian code clerks in their simplicity made many careless mistakes. When the structure of the code offered them two or more key numbers for the encipherment of the pages and lines of the code, they rarely made use of the possibilities and always took the same key number so that the disguise of the cipher and of the code was lost.

But even the cipher section in Moscow which prepared the cryptographic systems did not pay attention to all the little things which are very important for the solution of codes. For instance, it happened with almost every code that frequent letters or syllables stood on the same lines of different pages. These parallels could be traced in each new encipherment and immediately led to the recovery of several groups of the code. It may be that these parallel positions resulted automatically in the production of the code but the cipher section in Moscow should have paid attention to the matter, fortunately for the cryptanalyst, however, this did not always happen. It might almost be said that no matter how one human spirit exerts itself to be clever and sly in such matters, another human spirit which is concerned with solving the problem will always ferret out gaps and careless practices which can help it succeed in its task.

The cipher section in Moscow committed a gross error when it permitted the cipher sections of the various units to construct local codes, i.e., those codes which were to be used by the smaller units of the army. These smaller cryptographic units received from the central office in Moscow directions and models for the newly conceived codes and they were supposed to follow these models. They were free to choose the code elements themselves, to determine the number of groups and to set up the encipherment according to a system which they were to work out.

As a result it was observed during the war that many air armies, RAB's and BAO's (subordinate units of the air armies) always had codes of the same type which differed only in their vocabulary and encipherment.

These codes which were set up by the units themselves were not supposed to be in use for longer than three or four weeks. At the expiration of this time the cipher sections of the units were to see to it that the codes were changed. The reason for this was probably that the cryptographic center in Moscow had figured out that after this length of time codes of a simple character could no longer afford security and must therefore be replaced by new ones.

But even this rule was not always followed. Many codes remained in use for longer than four weeks or, inexplicably enough, were used alongside the new code.

This facilitated the decipherment of the new code because it was possible to compare decrypted messages in the old code with the messages in the new code.

Not infrequently it happened that one unit enciphered the message by a new code and sent it to another unit which did not yet have the new code. This second unit would then request in the old code a repetition of the message in the code it held and the request was granted. The two messages, one in the new and one in the old code, were compared by the cryptanalytic section. It usually turned out that the number of groups in the two messages was identical, hence the same text had been enciphered in the same way; whereupon the decipherment of the message in the old code resulted in the solution of the new code.

It is clear that the enemy intercept service not only clung obstinately to the decryption of the messages but gave heed to every trifle, in particular to careless mistakes. And these trifles, which seemed of no importance to the Russian cipher clerk, frequently betrayed a great deal. In the long years of his practical work the cryptanalyst not only became acquainted with the types of codes and ciphers used by the Russian cryptographic service, he also became acquainted with the mentality of the Russian radio and cipher personnel, learned to know the mistakes that may be made in enciphering messages and gave his entire attention to all those

things which would facilitate his work. The Russian code clerks surely contributed their share to the facilitation of his work during the war.

The practice of the Russian cryptographic service during the war of allowing each unit to use its own code instead of having a few large difficult codes for all units of the army had its advantages and disadvantages. The advantages were too slight to fully justify the practice. It merely cost the enemy intercept service more labor. It might have been all right if the Russian cryptographic personnel had been better trained and if the codes had been replaced regularly as intended. But this did not happen. The disadvantages were out of all proportion. The relatively easy codes, which were made easier to solve by the failure of the poorly trained personnel to obey instructions and by their errors, could be worked out and decrypted quite adequately. Furthermore current solution of the code made it possible to determine the location of the units which used them.

It is a question as to whether all this can be avoided in the future and whether the codes can be replaced without exception by machine ciphers. With the higher echelons, which are usually fairly stationary, this may well be the case. But equipping all mobile units of the army with a cipher machine is too dangerous and would require hundreds of machines. For this reason the Russians will hardly be able to do so. There are other reasons for coming to this conclusion: if a cipher machine falls into the hands of the enemy it cannot be replaced as easily as can a code; furthermore it is not so easy to transport as a code or a table which can be carried in one's pocket; the cipher machine cannot be destroyed easily as can a code; and it must be operated by well trained personnel such as was generally not available in the Red Army down to the close of the war.

It is hard to say what paths the Russian cryptographic service will choose-or perhaps has already chosen-for its communications after having learned about the work of the German cryptologic service from captured documents or the statements of captured intercept personnel.

It may be assumed that the Russian units which have their fixed locations in the East Zone, Poland and other occupied countries will transmit their messages by wire for the most part. In war time, or even in the case of major maneuvers this will scarcely be possible. This could be observed

frequently even before the war. Although radio traffic is very heavy in connection with maneuvers, it could also be observed between maneuvers, when the actual transmission of information was by wire and radio communication was maintained merely for practice purposes without sending many actual messages.

Since during the war units of the army are constantly in movement, no other means of communication will be as swift and sure as radio and consequently will be enciphered by manual codes and ciphers of all types.

It may be that better planned codes and ciphers are already being employed extensively and that decipherment will be more tedious and more difficult. But thus far whatever a human spirit has devised and made practicable some other human spirit has always solved. Even though in the future this will require more time, still cryptanalysts will solve the new types of codes because little careless mistakes will continue to be made and even difficult codes can be solved with the aid of these errors.

It is to be regretted that after the end of the war the Germans were not permitted to continue their intercept activity and that now there has been an interruption of over 6 years in the contact it maintained with the Russian cryptographic service.

The specialists who were engaged in this scientific work for many years have been inactive and will hardly be able to pick up the broken thread if their services are again required. But they do have years of practical experience behind them and they know the mentality of the Russian radio and cipher personnel which will surely not change and they would be able to reestablish the broken contact.

Even though the intercept service did not do much with the new traffic, there will still be enough to make evaluation worth while.

A modern army without a smoothly functioning and well organized radio intercept service is no longer conceivable. The intercept service provides the command staffs with valuable information regarding the neighboring country and secures its own country against unpleasant surprises.

End of Part II.

PART III

PHOTO EVALUATION

In spite of the fact that the German Command Staff got a fairly clear picture of the Red Army as a whole, its organization, composition, strength, distribution over various areas, etc., and was able to make proper dispositions before military action began, the German troops had some big surprises in store for them as they moved forward into the extensive territory of Russia.

Of course it was known that the roads of the Soviet Union could not be compared with the roads of other countries. Save for a few great highways, the roads of Russia were in poor condition and not always passable. But any exact knowledge of the caracteristics of the terrain as a whole as it really was at the different seasons of the year was completely lacking.

In all other countries one could study the entire country in detail before the war. Foreigners who visited a country could move about freely and photograph anything they wished to (except special factory and harbor installations). It was a different story in the Soviet Union. Since it came into being, this country had been surrounded by a high wall. Not many travelers moved about freely in this enormous country and still fewer were allowed to take photographs. Those photographs which were made in the Soviet Union or could be purchased were so unimportant that one could do nothing with them.

Agent reports which came only sparingly from Russia were concerned primarily with spying out other secrets such as manufactures and armaments, strength of the Red Army and its plans and matters of diplomatic or political moment. Even the air reconnaissance carried on during the war in the unoccupied areas of Russia and the countless aerial photographs taken did not give the Command Staff an exact survey of the various types of terrain and the true condition of main and subsidiary roads under different weather conditions.

From the aerial photographs taken continuously in occupied and unoccupied areas of Russia the German Air Force compiled a pictorial atlas which in its way was exceedingly valuable. One aerial photograph was joined precisely to the next and constituted an atlas which could afford a good survey of the country as a whole without betraying details of the terrain. Not until German troops had penetrated far into Russia and photographed practically everything that the armed forces considered necessary, could one see what the huge Russian territory looked like from north to south.

Of course those things were photographed primarily which were of interest to the individual German soldier whether he were a private or an officer. He did not make his exposures to create a valuable pictorial document but to paste them in his album later on as a souvenir of the time of the Great Struggle and of his sojourn in Russia. A few took delight in photographing supply trains abandoned in the mud, wide desolate plains, little tumbled down villages, bridges and cities which had been destroyed, the areas where great battles of encirclement had taken place. Others, who had the good fortune to stay for some time in beautiful towns and cities, turned their cameras on beautiful landscapes, arms of the sea, river courses, airfields, mountain ranges and other worthwhile targets. Thousands of pictures were taken which showed the country as no one else had ever seen it. Pictures were taken at all seasons and in all weathers, some good and some bad but in any case very interesting.

It is natural that many more pictures were taken in Southern Russia than in the Central Sector and that there were still fewer taken in the North. In the Northern Sector pictures always showed the same line and the same objectives. There were Baltic cities like Riga and Reval, then Pskov, Novgorod, the area around Luga and Leningrad. There was the Dünaburg-Pskov-Luga-Leningrad highway and the area along Lake Ilmen. There was not much to take. The area was desolate and dreary and the Northern Sector was not very great. "Not much happened there" and consequently not much could be fixed in photographs.

On the Central Sector it was already different. But even there it was usually the same areas which were photographed: the highway with the cities Minsk, Orsha, Smolensk, Vyazma; the areas and cities where great encirclement battles occurred like Vitebsk, Juchno, Bryansk Bobruisk and the area around Moscow. In general the photographs showed villages and cities that had been shot to pieces, great open landscapes, highways and the poor roads with little unpretentious hamlets in summer and in winter. Cities like Minsk, Smolensk and Vitebsk were photographed in all possible variations and from all directions by those men who were stationed there for some time.

A rewarding target was afforded by the Southern Sector, in particular the Crimea with its marvelously beautiful resorts on the Black Sea and the Caucasus with its coasts, its mountains and its ravines. The German soldiers, railway officials and members of technical sections occupied in the south with the restoration of damaged rail lines, factories, bridges and storage dams, had time to take everything that came within range of their lenses. Dnepropetrovsk, Zaporozh'e with its great storage dam, the beautiful large Ukranian cities Kiev, Odessa, Poltava and Vinnitsa, where OKH was located for a long time, Kharkov, where the great tractor and tank factories were visited and restored, the oil area around Maikop in the Caucasus, and then the roads, neat pretty little villages, great rivers like the Dnepr, Don and Bug with bridges - both intact and destroyed, and even the famous city of Stalingrad with the Volga showed up in countless pictures.

All these pictures were later collected and evaluated. The attempt was made to get as much as possible out of these amateur pictures and to reconstruct from single photographs a comprehensive pictorial atlas which would show everything as seen from the ground. These unhoped for pictorial documents, which were not intended for evaluation purposes, yielded far more than all the agent reports and aerial photographs taken together. They showed the country with its different terrain characteristics, its cities and smaller localities, as no one had ever been able to see them previously.

Had this photo-evaluation and the resulting pictorial atlas been available before the German-Russian war the German troops and especially Supply would have had an easier time of it. They would have accommodated themselves to the situation and been able to overcome the difficulties that confronted them at every turn.

How this photo-evaluation was conducted is shown by the following report with a few sample pictures.

Photo-evaluation and
orientation of the exposures.

All the collected photographs were sorted according to the several cities, villages and small areas. City maps on a scale 1: 25,000 were prepared for the various cities and those photographs which could be described were located therein.

In general the squares, churches, public buildings, rivers with highway bridges and the principle streets were photographed in the larger cities. Most of these could be marked on the city maps and consequently could be found and their location determined in the snapshots.

Precise orientation was entered in the form of a red arrow on the chart. The beginning of the arrow, which was marked by a cross, indicated the place from which the picture was taken while the direction of the arrow showed the direction in which the camera was pointed. All the arrows of a series of pictures (e.g., of one city) were numbered serially and the exposures were numbered correspondingly. All exposures from one city were put together so as to tie in with one another as far as possible. Each picture was described precisely and the direction in which the camera was pointed was indicated. Special characteristics were described, e.g., the type of pavement of the streets, broad much traveled streets in the business section, etc. (See Example 1).

It often happened that a number of pictures taken by different persons showed one and the same thing. The target was usually shot from different

but also show the characteristic landscape by which its general situation can be determined.

positions so that comparisons and observations could be made. Furthermore from the many pictures of one and the same object, each described by the individual in his own fashion, it was possible to check whether the data agreed in general or not. Those pictures which appeared doubtful, e.g., landscapes which could not be described and interpreted precisely, were collected separately and compared with other pictures of the same area. Now and then it was possible to recognize a landscape by special features and other pictures that could be oriented in which case the poorly described ones could also be located in useful fashion.

A picture was usable if it could be accurately located within two kilometers. A deviation of two kilometers did not matter very much because the countryside did not change essentially within a radius of two kilometers.

City pictures were important if they showed churches, large public buildings, river crossings, squares with little parks, and large main streets which left their imprint on the physiognomy of the city. It was necessary that these objects be described and that it be known whether they were in the center or in the southern, western, northern, eastern portion of the town. Here again the number of exposures of the same object could result in precise orientation.

When the direction in which the camera had been pointed could not be stated the evaluators tried to determine it themselves. If the exposure was made on a sunny day, the direction could be determined by the shadows.

Landscape pictures were oriented in the same fashion, the red arrows had to show in the same fashion the point at which they were taken and the direction. The description of the landscape must also be precise. It is important to know the character of the soil at different seasons and in different weather.

Aside from city maps all other exposures were entered on the German army map 1: 300,000. (See Example 2)

In Example 3 are shown other picture evaluations with orientation. These single pictures selected from various areas not only show whether the region is flat or with elevations, whether it has good or poor road facilities, but also show the characteristic landscape by which its general situation can be determined.

In Example 1 various exposures from Vinnitsa and Odessa have been evaluated and oriented. All pictures of Vinnitsa came from different individuals who had given their pictures only brief descriptions. E.g.:

"bridge over the Bug in Vinnitsa in the eastern part of the city".

"street running up through town toward the north".

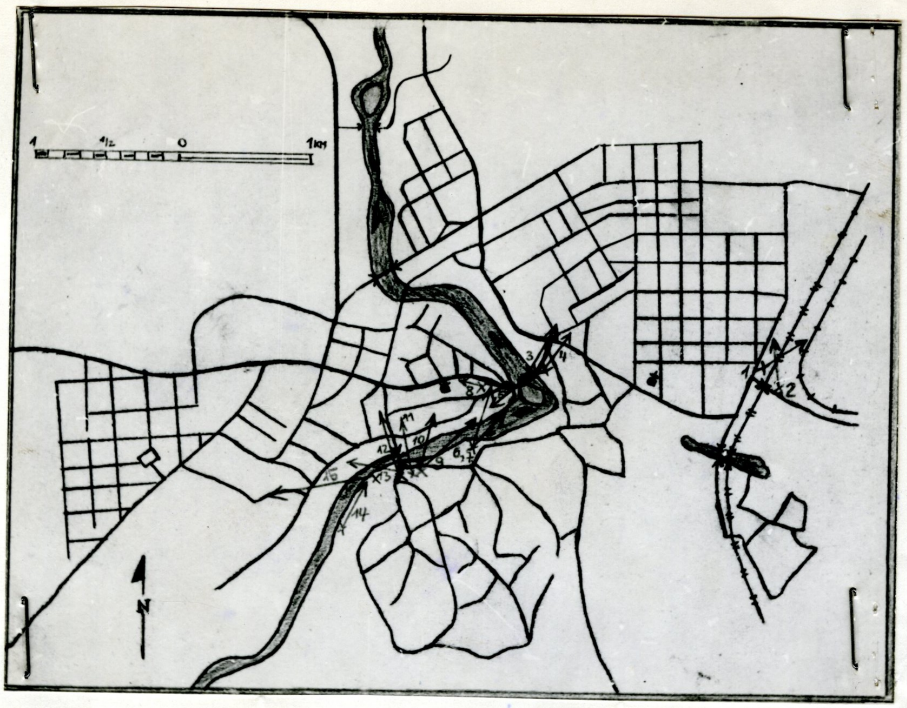
the picture evaluator had to study all the pictures carefully, had to describe every little detail which could be seen in the pictures such as striking buildings, towers, churches, river bends, heights, street locations, etc. He looked for similar objects in the other pictures and was thus able to recognize connections between these several pictures and to orient them correctly.

It often happened that the data with respect to directions on the pictures were false because they could not be harmonized with the lighting and the indicated situation. But usually it was possible during evaluation to find the correct place on the map by comparing streets, squares, churches and river courses.

The picture evaluator had to expect that those taking the pictures could not have described them precisely. The reason for this was not hard to find because the pictures had been taken for the person's own use rather than for evaluation purposes and the person could not remember later whether he was looking NNW or NW or simply to the North at the time. Furthermore many of the pictures were taken early in the war during the German advance so that one did remember the locality and the subject of the photograph perfectly well but did not recall the exact point in a given area.

Pictures which afforded no precise data were not accepted for evaluation even though the subjects were interesting.

Here is an example of evaluation and orientation of pictures of Vinnitsa and Odessa.



Example 1

Vinnitsa (Scale 1: 35,000)

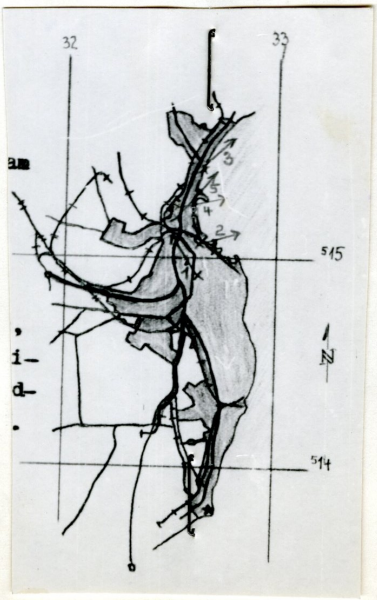
City on the Bug in Southern Ukrania. Less than 100,000 inhabitants. No special industries. To the south of the city along the Bug are several considerable elevations. The city was not badly destroyed during the war.

Plan of the City of Odessa

(Scale 1: 250,000)

Note: Large Ukrainian city on the Black Sea 640,200 inhabitants.
University and other schools of like rank, museums, shipyards, heavy machine industry, chemicals, petroleum.

For photo evaluation with the same numbering see Supplement I (Special map).

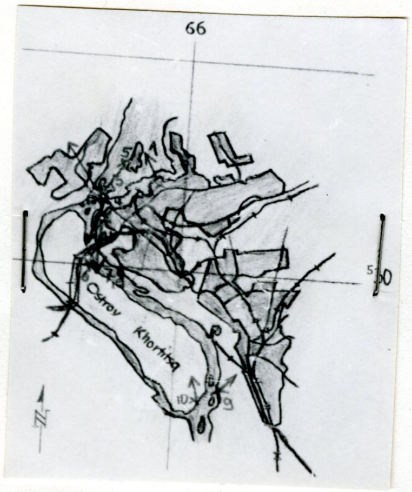


Example 2

Zaporozh'e and Vicinity

(Scale 1: 250,000)

Note: Zaporozh'e, formerly Alexandrovsk on the Dnepr, 190,000 inhabitants, metal smelting, storage dam partially destroyed during the war and repaired. For picture evaluation with the same numbering see Supplement I (Special map).



Note: Pictures 2 and 3 were taken across the storage dam looking toward the west bank (to the NW). Picture 4 was taken toward SW across the sluice at the storage dam.

Picture 5 was taken from the Dnepr looking SW toward the storage dam.

Picture 6 looking to the NE toward the railway bridge.

Pictures 7 and 8 taken from the western part of town looking south across the Dnepr toward the railway bridge.

[Translator's note: The actual photos were not included by von LINGEN, but the sides from which they were taken are indicated by numbers on the above map.]

SECRET

Vinnitsa

Vinniza G

Abschnitt - Süd

1 Frontansicht vom Bahnhof Vinniza im O der Stadt mit dem Blick auf d.gr.Bahnhofsplatz nach NO.

2 Bahnanlage und Bahnhofsgebäude über die Gleise und offenen Bahnsteig nach N aufgenommen.

3 Blick vom zweiten Teil der Hlozdoppelbrücke über d.Bug (siehe auch Bild 5 u.6)stadteinwärts nach N.Nach rechts biegt die Uferstr.mit Strassenbahngleisen.

4 Blick auf dieselbe Strasse stadteinwärts wie Bild 3 mit der Einbiegung in die Uferstr.nach N.

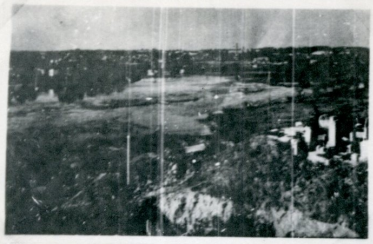
5 Blick auf den zweiten Teil der Doppelbrücke und den östl.Teil der Stadt von der Holzbrücke aus nach SW.

6 Blick von einer Anhöhe auf die Doppelbrücke nach O.Der auf dem Bild sichtbaren forderen Teil der Brücke geht zu der Uferstrasse (s... Teil de... im Bo... ptstr.

7 Von derselben Stelle wie Bild 6 in gleiche Richtung aufgenommen.Rechts im Hintergrund das Bahnhofstgebäude.

8 Die Hauptstrasse in Vinniza die nach SO zu der Brücke führt.Die Strasse hat öffentl.Gebäuden und grosse Hotels.

SECRET

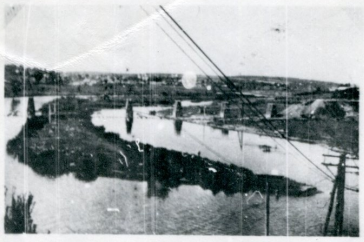


9 Blick vom hohen westl.Ufer der Bug auf die Doppelbrücke nach NO.Im Vordergrund unter der Anhöhe die Uferstr.die zu der Doppelbrücke führt.

10 Von derselben Anhöhe wie Bild 9 über den Bug auf den NO-Teil der Stadt aufgenommen.Unten diesslbe Uferstr.die z.d.neuen Brücke

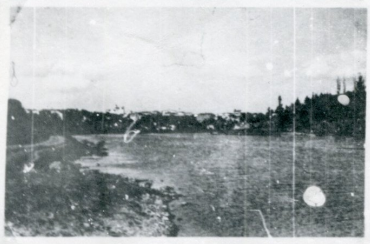
11 Vom hohen westl.Ufer,weiter westwärts auf die Stadt und die neue Brücke nach N aufgenm.

12 Blick auf diesselbe neue Brücke von gleicher Anhöhe nach N.Die Strasse v.d.Brücke mündet in die Hauptstr.im Zentrum der Stadt.



13 Zerstörte alte Brücke über den Bug von der Anhöhe wie Bild 11 nach NW aufgenommen.

14 Vom linken Bugufer über den Fluß auf die Stadt nach NW aufgenommen.



15 Bug südwestl.von Vinniza mit dem Blick flussauswärts auf den südl. Teil der Stadt aufgenommen.

Translation of Captions of the Pictures
of Vinnitsa on the Preceding Pages.

1. Front of the Vinnitsa station in the eastern part of town looking NE at the station square.

2. Station and station building looking N across the tracks and open platform.

3. View from the ssecond portion of the wooden double bridge across the Bug (see also pictures 5 and 6) looking N towards the center of the town. Uferstrasse with street car line turns off toward the right.

4. View to the N showing same street as in picture 3 with the junction of Uferstrasse.

5. View from the wooden bridge to the SW of the second portion of the double bridge in the eastern part of town.

6. View from the height towards the E towards the double bridge. The portion of the bridge visible in the foreground leads to Uferstrasse.
[Three lines covered by picture 8.]

7. Taken from the same position as picture 6 in the same direction. The railroad station is to the right in the background.

8. The main street in Vinnitsa which runs SE to the bridge. On the street are public buildings and large hotels.

9. View from the high western bank of the Bug on the double bridge towards NE. In the foreground below the height we see the Uferstrasse which leads to the double bridge.

10. Taken from the same height as picture 9 across the Bug towards the NE part of the city. Below we see the same Uferstrasse which leads to the new bridges.

11. Taken from the high western bank further to the W towards the city and the new bridge to the north.

12. View of the same new bridge from the same height towards the N. The street from the bridge runs into the main street in the center of the city.

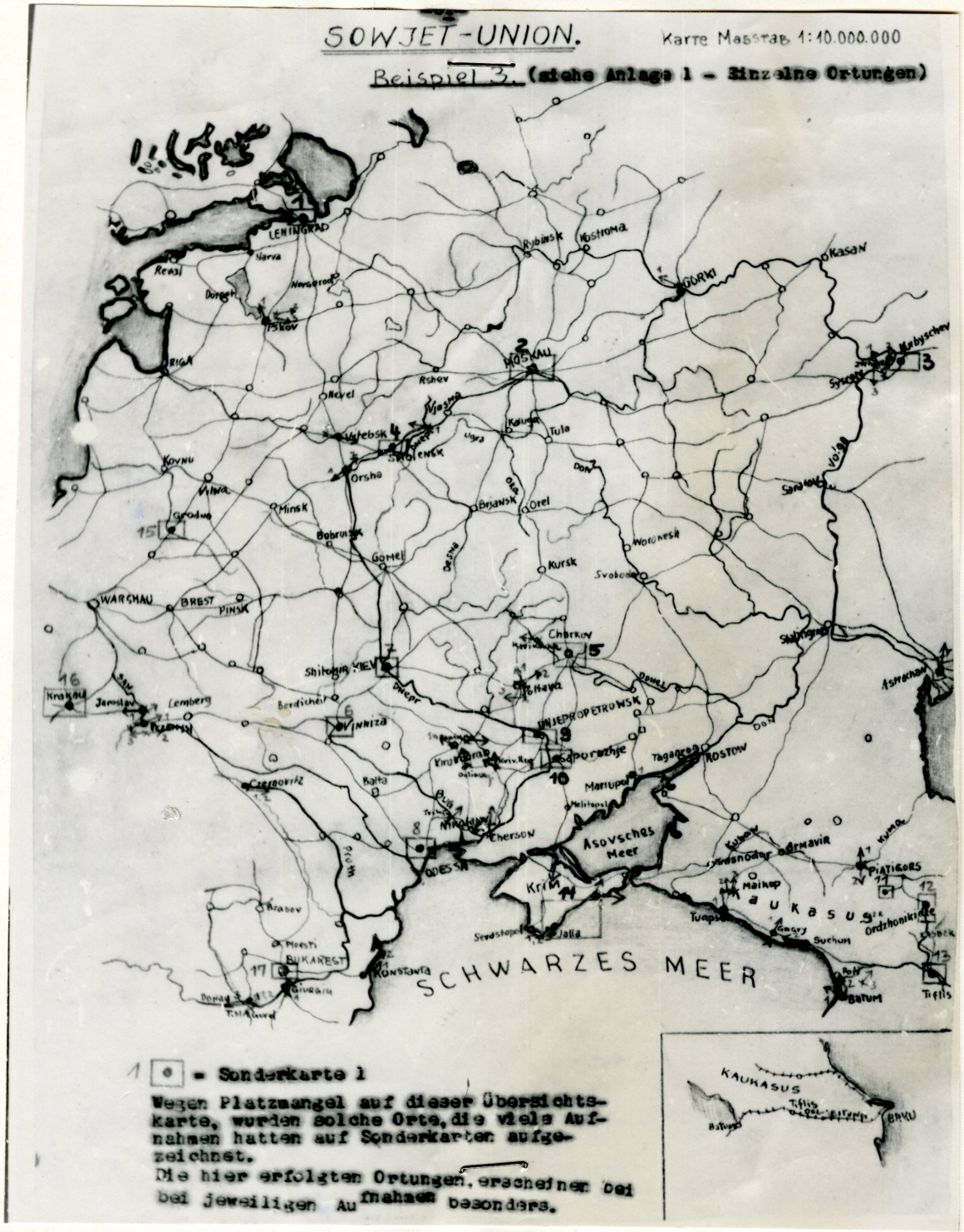
13. Destroyed old bridge across the Bug taken toward the NW from the height as in picture 11.

14. Taken from the left bank across the river towards the city to the NW.

15. The Bug SW of Vinnitsa with the view downstream towards the southern part of the city.

Example 3. (See Supplement I - locations)

The Soviet Union. (Scale 1:10,000,000)



1 ⊡ = Special Map 1.
Because of the lack of space on this map those places, which had many photos, were drawn on special maps. The locations shown here appear especially often in the present pictures.

All these orientations were made on maps of the Soviet Union (German Army Maps scale 1: 300,000). The pictures singly and in series were given the number of the map on which they were entered.

In Example 3, additional pictures are given with descriptions and orientation. They have been taken from various regions and, like the preceding example, show striking characteristic of the cities and the towns and the landscapes.

This little collection comprising only a part of the pictures from the same areas reveals at first glance both interesting and uninteresting pictures, each of which yielded some contribution to the total survey of the area. Even the pictures which at first appear uninteresting supplied vauable details for the compilation of the pictorial atlas.

These samples merely show a partial evaluation of a few pictures which suggest only special characteristics and the general situation. Final evaluation took place later after all the pictures had been collected. It treated more precisely the pictures in the cities and towns, the character of the landscape, the position of streets and striking features, the structure of bridges, railway installations and factories. Every bit of land and every target that was photographed could not only be oriented but could also be evaluated in a very precise manner.

Pictures of cities and towns such as Leningrad, Moscow, Kujbishev and places along the Volga, the military highways in the Caucasus, Tiflis and Baku camefrom people who escaped to the Germans during the war or from the Russian population in the occupied area. Only such pictures were accepted as were made not earlier than 1938.

The cities, villages, factories, bridges and railway lines were constantly being expanded and were changing their looks and their location. For this reason no very old pictures could be used. On the other hand mountains, coast lines, river courses and simple landscapes did not change in the course of years and here pictures might be somewhat older although the limit was set at 1925.

Special interest attached to these pictures from the unoccupied portions of Russia because they were rare and very important.

Of course evaluation was more difficult because the pictures could not be described fully. But since the objects were generally of considerable size and fairly well known, these pictures could also be oriented satisfactorily after careful checking.

Gradually from the thousands of pictures a pictorial atlas emerged. Some cities and areas had been so often photographed that an almost complete picture could be obtained. Other places were recorded by few photographs, many by none at all, so that these places could only be represented and evaluated in part if at all.

All in all, however, valuable results could be achieved by this picture evaluation and much that had hitherto been completely concealed in the isolated country was revealed clearly, exposing many secrets of a peculiar country which is still trying to keep to itself all of its own characteristics.

Any evaluation, whether of decrypted radiograms or from pictorial documents, must be absolutely reliable. The evaluator must not be allowed to weave in any opinions of his own. He must stick to what he has in black and white, then his reports and evaluations are really dependable. Whenever he has made discoveries of his own during his work, he can present them in writing, but it must be perfectly evident that these remarks are his own.

CONCLUSION

It need not be a preparation for war if one observes his neighbor in all possible details and thus becomes acquainted with his strength, his weaknesses and his intentions.

It is a mistake if a country does not do this. Each country must have even in peace time a well organized and smoothly functioning intercept service. This does not call for a great effort and by so doing one's own country is insured against unwished for surprises which can have more serious results when they come unexpectedly.

There are only a few specialists in this field. The cryptologic service is a science apart but years of experience have shown that these few specialists can accomplish much.

During the two World Wars this scientific work never failed and it rendered valuable service. One ought not to pass over this fact lightly and fancy that in our atomic age this work has become superfluous. All other security measures loose much of their value if thoughtlessly or out of ignorance the intercept service is neglected.